Universidade Federal de Santa Catarina – UFSC
Centro Sócio Econômico - CSE
Departamento de Economia e Relações Internacionais

CRISTÓBAL ALONSO CÁRDENAS ORLANDINI

CRIPTOMOEDAS COMO ALTERNATIVAS PARA O MERCADO DE TRANSFERÊNCIAS E PAGAMENTOS

Florianópolis, 2017

CRISTÓBAL ALONSO CÁRDENAS ORLANDINI

CRIPTOMOEDAS COMO ALTERNATIVAS PARA O MERCADO DE TRANSFERÊNCIAS E PAGAMENTOS

Trabalho de Conclusão de Curso apresentado ao Departamento de Economia e Relações Internacionais, como parte dos requisitos necessários à obtenção do título de bacharel.

Orientador: Prof. Dr. Roberto Meurer

Florianópolis, 2017

CRISTÓBAL ALONSO CÁRDENAS ORLANDINI

A Banca Examinadora resolveu atribuir a nota 9,0 (nove) ao aluno Cristóbal Alonso Cárdenas Orlandini na disciplina CNM 5420 – Monografia, pela apresentação deste trabalho.

Banca Examinadora:

_____

Prof. Dr. Roberto Meurer
Orientador

_____

Prof. Dr. João Rogério Sanson
Membro da Banca

_____

Pedro Bueno de Almeida
Membro da Banca

RESUMO

Ao surgirem como um método inovador para a realização de transferências de fundos e pagamentos, as criptomoedas cada vez mais passam a ocupar um numero maior de espaços nas discussões que tangem a economia. Com fortes opiniões dos lados opostos e com um período de vigência relativamente curto, há muito a se discutir a respeito dos riscos, benefícios e viabilidade destas novas moedas digitais. Acompanhado por um discurso de rebeldia anti-estatal, as criptomoedas já se credenciaram tanto como o maior símbolo de liberdade de seus adeptos, quanto como alvo de pesadas críticas e desconfiança dos meios tradicionais do segmento das finanças. Embora muitos assuntos pareçam ainda consideravelmente nebulosos, negligenciar a atividade destes novos meios de pagamento – independente da visão ideológica – é negar a discussão de um tema cada vez mais recorrente na sociedade: a viabilidade e as consequências dos impactos do rápido progresso tecnológico no dia-a-dia. Anunciando-se como métodos descentralizados de transferência de dinheiro, alheios a qualquer controle estatal e com potencial para permitir que os indivíduos negociem e façam trocas sem a necessidade de um intermediário, a viabilidade das criptomoedas como concorrentes ao dinheiro estatal tem gerado discussões a respeito de um tema não muito atendido nos últimos tempos, o surgimento de moedas privadas como uma opção real e confiável. O que esta pesquisa tentou demonstrar é que estes novos instrumentos possuem características que as credenciam como inovadoras, mas que, tanto por adversidades internas quanto externas, ainda encontram dificuldades para serem inseridas como ativos capazes de concorrer com as moedas estatais, e que por não parecerem, até a data da finalização deste trabalho, ferramentas sustentáveis para transferências e pagamentos, correm o risco de não conseguirem corresponder aos anseios de seus usuários e apoiadores.

PALAVRAS-CHAVE: Criptomoedas; Bitcoin; Moeda privada.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 TEMA E PROBLEMA DE PESQUISA

É possível dizer que, hoje, o maior facilitador de comunicação e logística humana é a Internet. Esta ferramenta permite que a população tenha cada vez mais acesso a informações capazes de mudar sua rotina de vida. Seja através de videoconferências ou aplicativos de transporte privado, o dia-a-dia do cidadão comum está cada vez mais interligado aos meios digitais. Mas como esta mudança de paradigma afeta o mercado de pagamentos e transferências de fundos? São, nestas atividades presentes em todas as localidades do mundo, que esta pesquisa se centralizará.

Sob o véu desta sociedade cada vez mais informatizada e estabelecida em redes, diversas alternativas começam a surgir. A população, cada vez mais cética em relação aos grandes aparatos financeiros-estatais, começa a se mobilizar a fim de encontrar alternativas aos sistemas vigentes.

É neste contexto de incerteza e dúvida em relação às efetivas intenções das clássicas instituições financeiras, que surge uma ameaça ao seleto grupo composto por estas instituições: o nascimento das criptomoedas.

Embora sua maior bandeira seja o Bitcoin[1], várias moedas digitais completamente descentralizadas de qualquer rede governamental, estão surgindo como opção para a população receosa de que as políticas adotadas pelos Bancos Centrais e instituições financeiras não sejam as mais adequadas; abordando tanto pelo ponto de vista da reserva de valor, quanto pelo da privacidade e autonomia de realizar operações financeiras.

O governo da Índia, recentemente, se inclinou de maneira favorável a restringir a movimentação de dinheiro físico. Como reportado pela CNBC (Novembro de 2016), de maneira inesperada, o governo tomou medidas para incentivar os meios digitais de pagamento em detrimento do dinheiro físico, sob a justificativa de combate à lavagem de dinheiro. Desta forma, o Estado retirou as notas de 500 e 1000 rupias de circulação, criando um clima de incerteza na população do país. Seria mesmo um combate genuíno à lavagem de dinheiro, ou

[1] Como explicado no artigo “What is Blockchain Technology? A Step-by-Step Guide For Beginners”, do site www.blockgeeks.com, o Bitcoin é uma moeda virtual descentralizada, que opera através da tecnologia *blockchain*, que funciona como uma cadeia cujo protocolo de criptografia evita que sua informação seja corrompida, totalmente movida por algoritmos pré-definidos. Esta cadeia é construída por uma rede P2P (*peer-to-peer*), ou seja, cada dispositivo com acesso a Internet funciona como receptora e provedora de dados que delimitem o valor de determinada transação.

apenas mais um mecanismo para aumentar o controle sobre a população, visto que transações digitais centralizadas são mais fáceis de serem rastreadas? De qualquer forma, a resposta foi interessante: observou-se um aumento significativo do interesse por bitcoin no país, com a busca online pelo termo "bitcoin" chegando a seu auge histórico, como foi evidenciado pela ferramenta Google Trends[2].

Tudo isto traz de volta para a cena teórica econômica um debate adormecido (se é que alguma vez foi realmente despertado) a respeito das moedas privadas como solução para descompassos feitos pelos Bancos Centrais e/ou para os métodos complexos de transferência de fundos das instituições financeiras vigentes.

Hayek (1976) faz uma defesa ferrenha da abolição do Estado como emissor único de moeda e se posiciona a favor de um mercado de emissores que, incentivados pelo lucro, como em qualquer outro empreendimento, acabariam por aperfeiçoar as suas moedas, buscando atingir um público cada vez maior de adeptos. Ele argumenta que as decisões que tangem à política monetária das nações deveriam ser destinadas às instituições financeiras com fins de lucro, que conseguiriam dar uma estabilidade maior à economia, diferentes de uma instituição única como o Banco Central, onde as pressões políticas afetam as decisões de maneira corriqueira.

Um pouco mais tarde, White (1999) colocará para análise diversos argumentos que questionam a soberania do Banco Central como emissor único de moeda. O autor cria paralelos entre a *fiat-money*, a *commodity-money*, o padrão ouro e um mercado movido por instituições que emitam suas próprias moedas de maneira privada.

A premissa da pesquisa não se sustenta em uma discussão ideológica a respeito da atuação do Estado sobre a liberdade individual. Este debate requereria um espaço muito maior para resolver uma questão bem mais profunda, o que não é o objetivo deste trabalho.

Dito isto, esta monografia busca apontar os meios com que as criptomoedas poderiam surgir como alternativas para a realização de transferências e pagamentos, o viés descentralizador que as criptomoedas possuem e suas vantagens e desvantagens em relação aos métodos vigentes, usando como contexto teórico o que há na literatura a respeito de moedas privadas hoje.

[2] Dias após a decisão por parte do Banco Central de retirar as notas altas, os pedidos por Bitcoin aumentaram entre 20% e 30%. De maneira análoga, as buscas pelo termo "bitcoin" atingiram o auge histórico até então, logo na semana seguinte à decisão, segundo dados do Google Trends.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Apresentar as características das criptomoedas como alternativas para os instrumentos vigentes de meios de pagamento e de transferência de fundos e analisar sua viabilidade no contexto atual.

1.2.2 Objetivos Específicos

- Conectar o que a teoria econômica diz a respeito de moedas privadas com a discussão das criptomoedas hoje.
- Analisar a situação atual das criptomoedas e se seus comportamentos presentes correspondem às premissas anunciadas por seus idealizadores e apoiadores.
- Comparar as soluções de pagamento e transferências de fundos das criptomoedas com as usadas hoje.

1.3 JUSTIFICATIVA

Negligenciar o potencial das criptomoedas/moedas digitais descentralizadas como uma alternativa ao método convencional de operações financeiras é fechar-se para uma possibilidade de quebra de paradigma de suma importância. Não é mais possível omitir a capacidade que estas novas ferramentas têm para impactar a realidade dos meios de pagamento e transferência de fundos.

Desta forma, o primeiro capítulo buscará trazer um pouco do que há na teoria econômica a respeito da discussão de moedas privadas e do que caracteriza a reserva de valor em um ativo. Para discutir as moedas privadas, os principais autores estudados foram Friedrich Hayek e Lawrence H. White. Ao considerar a questão da reserva de valor, as adições de John Maynard Keynes ao tema também foram discutidas.

No segundo capítulo, se discute a origem do bitcoin, a principal criptomoeda já lançada até agora. Buscou-se criar um nexo entre os primeiros projetos de moedas digitais com o bitcoin e como este último utilizou muito das ideias destes projetos para definir a sua forma e viabilidade. Também se discute o seu funcionamento e como seu protocolo opera a fim de realizar transferências e pagamentos. Além disso, se inicia uma discussão acerca do valor de uma criptomoeda, ou seja, o que tornaria uma criptomoeda atrativa ou não.

O terceiro capítulo se destina à discussão da viabilidade das criptomoedas, considerando as suas possibilidades de inserção no mercado e os fatores que impediriam elas de se manifestarem como uma moeda capaz de concorrer com as moedas estatais. Discute-se também o relacionamento dos agentes dentro do protocolo e como a concentração de poder poderia afetar o atributo descentralizador do mesmo. Neste capítulo, é feita mais uma conexão entre os aspectos de reserva de valor que uma criptomoeda pode chegar a possuir e as opiniões de Keynes e White a respeito do tema.

O quarto capítulo foi destinado a discutir como a presença das criptomoedas pode influenciar o cenário atual de meios de transferência de fundos e pagamentos. Confronta-se a tecnologia *blockchain* das criptomoedas com o método SWIFT e também se discutem os custos de transação de ambos os métodos. Ao comentar sobre os custos de transação, se faz uma nova conexão com as ideias de Keynes e como as criptomoedas se comportam em relação ao que ele postula. Finalmente, entra-se em uma breve análise de como as criptomoedas podem influenciar camadas negligenciadas pelo sistema financeiro, incluindo suas virtudes e suas dificuldades.

O fato de não existir abundante respaldo na teoria a respeito das criptomoedas não deve ser motivo para adotar uma postura conservadora ao ponto de desestimular qualquer discussão a respeito. Muito pelo contrário, exatamente pelas discussões novas e pertinentes à realidade atual, é que se deve estudar mais a respeito destas novas ferramentas.

Embora também seja uma oportunidade de investimento, a mera análise desta nova modalidade de operações financeiras como "refúgio" de poder de compra é se limitar a um patamar muito mesquinho em relação ao potencial completo do mecanismo.

O avanço vertiginoso do progresso tecnológico tem revolucionado muitos setores. A popularização das criptomoedas lidará de frente com o modelo tradicional de moeda centralizada em um Banco Central, o que trará à tona uma série de debates entre a autonomia dos indivíduos e a atuação do Estado.

No entanto, o enfoque desta pesquisa se direcionará às atividades pertinentes aos meios de pagamento e transferências. Entrar em uma discussão ideológica a respeito do impacto social e político das criptomoedas tornaria obrigatório a especulação de caráter opinativo, o que não é o objetivo desta monografia.

2 MOEDA PRIVADA E RESERVA DE VALOR: REFERENCIAL TEÓRICO

2.1 O CONFRONTO DA MOEDA ESTATAL COM A PRIVADA

2.1.1 Conceito de *fiat-money*, o início da monopolização da moeda pelo Estado e suas consequências

O pilar primordial a ser discutido quando se fala em dinheiro ou moeda, é o seu valor. Não há como entender o valor intrínseco do dinheiro apenas analisando sua concepção física. Como White (1999) menciona, seja o bem ouro, pó ou sal, a sua utilidade física não se altera, nem afeta a importância do outro bem. A diferenciação existe apenas quando se lhe atribui um valor ao bem. É a partir deste momento em que a interpretação de importância que uma dita população dá a um determinado instrumento e que, por consequência, determina o seu valor, que o bem passa a possuir a alcunha de "dinheiro". A moeda estatal, como se conhece hoje, não passa de um pedaço de papel artificialmente injetado por valor. O valor da moeda consiste no que a sociedade acredita que ela vale. É esta moeda artificial que é conhecida como *fiat-money*.

Mankiw (2015, p. 220), define *fiat-money*:

> Dinheiro sem valor intrínseco é chamado de *fiat-money*. Fiat é uma ordem ou decreto, e *fiat-money* é o que é estabelecido como dinheiro por um decreto do governo. Por exemplo, compare as cédulas de dólares americanos (impressos pelo governo americano) e as cédulas de dólares do jogo *Monopoly* (impressas pela empresa de brinquedos Parker Brothers). Por que você pode usar as primeiras para pagar uma conta de restaurante mas não as segundas? A resposta é que o governo americano decretou seus dólares como o dinheiro válido. Cada cédula de papel na sua carteira diz escrito: "Esta cédula é moeda corrente para todas as dívidas, públicas ou privadas."

White (1999) defende que são as conveniências dos agentes econômicos que irão definir o valor da moeda, iniciando sua crítica ao ideário da corrente *mainstream*, de que a necessidade de um Banco Central é imprescindível para buscar estabilidade econômica. O autor comenta que o valor dos bens emerge naturalmente conforme for maior seu valor de atração.

White (1999) faz uma nova crítica ao poder acumulado dos Bancos Centrais e entra na discussão do *free-banking*, alegando que não existem evidências que provem a existência de

um Banco Central como fruto de um monopólio natural, mas sim da ideia artificial difundida em larga escala às populações de que o Estado é o único capaz de emitir moeda.

O Estado, ao monopolizar os meios de troca, retira a liberdade dos indivíduos de realizarem práticas que poderiam ser de maior comodidade a estes. Sob a justificativa de um governo que luta pelo direito das pessoas, a sociedade acabou perdendo um dos seus direitos mais importantes: o da liberdade de escolha. Ao delegar ao Estado o total e completo domínio de determinar o que é dinheiro "verdadeiro", os indivíduos forneceram um poder imenso a um grupo pequeno de burocratas que não estão alheios aos anseios da humanidade, como a garantia de retornos maiores, mesmo que ao custo da liberdade de terceiros, por exemplo.

2.1.2 Motivações, incentivos e causas da moeda estatal

Se existem dúvidas claras e bem fundamentadas a respeito da existência de um único emissor de moeda, é preciso entender o porquê deste paradigma permanecer vigente em todo o mundo. Por que as decisões em cima de políticas monetárias estão nas mãos de um pequeno grupo de pessoas?

É importante perceber que o Estado funciona como uma empresa. White (1999) afirma que, como em toda organização, os membros do Estado procurarão aquilo que mais lhes trouxer retorno e os maiores incentivos para isso. É o caso de uma taxa de juros estabelecida pelo Banco Central. Uma taxa que seja controlada pelo Estado permite que ele absorva enormes benefícios, visto que, exatamente por ser o proponente da medida, consegue antecipar movimentos da economia, o que para o autor é um dos objetivos do Banco Central. Obter o monopólio da taxa de juros é possuir a capacidade de gerenciá-la de maneira que melhor atenda os interesses desta organização.

2.1.3 Hayek e a defesa da emissão livre de moeda

Hayek (1976) faz uma crítica à concepção generalizada a respeito da necessidade de um governo ter plenos poderes para definir o volume da base monetária em determinada comunidade. Não é difícil compreender que esta visão seja ampliada para a totalidade dos países do mundo visto que, embora em alguns países o nível de autoritarismo seja maior, a noção de uma cúpula com um número reduzido de cabeças pensantes administrando e delegando as operações que tanjam às diretrizes econômicas, é válida para todos os países.

A defesa de Hayek (1976) para a emergência de uma concorrência benéfica de moedas se sustenta sob as premissas do livre comércio. A livre circulação de opções para a população, por

mecanismo natural de mercado, satisfaria a necessidade dos consumidores em escala progressiva e, por consequência, forçaria os emissores de moeda a tornarem seu produto cada vez mais atraente, visto que o objetivo do empresário sempre é o lucro.

Uma crítica clássica ao pensamento liberal de economia livre e concorrência aberta é de que, sob a falta de órgãos regulamentadores do Estado, a natureza do mercado acabaria erguendo monopólios, através de uma luta injusta e desigual entre os agentes econômicos. No contexto analisado neste trabalho, que é de um mercado livre de moedas, este bem não passaria despercebido. Mesmo autores de corrente liberal, favoráveis ao enfraquecimento do poder estatal, contrariam Hayek e seu método ideal de concorrência monetária. Friedman (1987) argumenta que não existem tantas travas para o desenvolvimento de novas moedas privadas como Hayek aponta. E que, mesmo sob este contexto, as mudanças de estrutura institucional não advêm de vontades dos indivíduos e sim de crises. Ele compara o estudo de moedas em concorrência com a adoção de taxas de câmbio flexíveis, dizendo que estas não tiveram grande impacto institucional na estrutura dos Estados Unidos.

Como Hayek (1976) sustenta, a população contemporânea nunca teve a oportunidade de estar integrada a um sistema de livre concorrência de moedas, logo, não é surpresa que a proposta do autor seja vista com olhos receosos e até debochados por parte da corrente teórica *mainstream*. Não há melhor contexto do que o atual para colocar esta teoria à prova. Com um mercado de criptomoedas cada vez mais imponente, possuindo uma capitalização superior aos US$100 bilhões e um volume de transações diárias superior aos US$ 2 bilhões – considerando apenas as duas maiores do mercado, Bitcoin e Ethereum – está ressurgindo um mercado de moedas privadas que há muito tempo estava adormecido. Embora o Bitcoin surja como bandeira principal das criptomoedas, dúvidas em relação a seu protocolo tem ocasionado o desenvolvimento e popularidade de novas criptomoedas, com protocolos próprios para atender demandas específicas do público.

2.1.4 White, Hayek e os incentivos para a criação de moedas privadas de qualidade

Como comentado anteriormente, White (1999) defende que o valor dos meios de troca está estritamente relacionado com seu poder de persuasão perante os indivíduos, o público usuário destes meios.

Para White (1999), por dinâmica de mercado, as instituições emissoras de moeda encontrariam tantos incentivos para aceitar diversos tipos de moeda, quanto para emitir moedas

fortes e competitivas. Uma instituição que aceitasse os mais variados meios de troca atrairia um maior número de clientes, passando a ganhar nome e prestígio entre as instituições.

De maneira alheia a esses anseios, o interesse em criar e manter uma moeda forte e útil, incentivaria os clientes a guardarem a moeda desta instituição, deste modo, apreciando-a. Isto poderia vir a resolver os problemas de expansões monetárias excessivas, por exemplo. Diferente do Banco Central, não existiria ganho para o proprietário da instituição financeira se este imprimisse valores extraordinários de moeda, pois viria a desvalorizar seu produto.

Hayek (1976) comenta que num mercado livre para emissores de moeda, as empresas envolvidas, por se motivarem pelo lucro, estarão sempre tomando medidas para que seu produto (moeda) esteja de acordo com os orçamentos e objetivos propostos pelo planejamento destas empresas e que também abasteçam os anseios do público-alvo. Contrário ao Estado, que, em alguns casos, para manter sua reputação, acaba tomando medidas radicais para postergar crises de contas públicas e acaba incrementando-as, as instituições financeiras tomariam cuidados para evitar estes erros, visto que as crises cairiam em cima delas mesmas, ao contrário das políticas monetárias governamentais, onde o ônus das medidas equivocadas sempre cairá com maior peso em cima da população como um todo.

2.2 A RESERVA DE VALOR

2.2.1 A incerteza em Keynes

As características de incerteza dentro de uma economia eram dignas de estudos aprofundados por parte de John Maynard Keynes. Para Keynes (1936), entender a importância das expectativas em um contexto de incerteza impossível de mensurar, significava uma oportunidade de explicar os comportamentos dos agentes econômicos de uma maneira mais simplificada, visto que em situações de economia mais estável, onde a incerteza é menor, a capacidade de gerenciar o risco se apresenta como mais facilitada.

Carvalho (2015), entende que, em contraste com a teoria apresentada por economistas neoclássicos, como John von Neumann e Oskar Morgesntern, onde o risco era considerado como uma consequencia das preferencias dos indivíduos, desde que as probabilidades das preferências pudessem ser mensuradas; Keynes abordava a questão por outro viés. Para Keynes, a ação dos indivíduos muda conforme a incerteza é maior, portanto outro método para considerar essas mudanças de comportamento era necessário.

Usando esta discussão como gatilho, Keynes viria a publicar sua obra de maior fama, *The General Theory of Employment, Interest and Money* (1936), onde o autor aborda os incentivos que levam um indivíduo a mudar seu comportamento sob ambientes de incerteza. Para apresentar suas ideias, Keynes introduziu três conceitos: a propensão a consumir, a eficiência marginal do capital e a preferência por liquidez. Ao falar da propensão ao consumo, Keynes estabelece seis fatores de influência dela:

1) Uma mudança na unidade de salário
2) Uma mudança na diferença entre renda bruta e renda líquida
3) Mudanças ocasionais em valores de capital que impossibilitem o cálculo da renda líquida
4) Mudanças nas taxas de câmbio entre bens presentes e futuros
5) Mudanças na política fiscal
6) Mudanças nas expectativas de renda presente e futura

2.2.2 A preferência por liquidez de Keynes

Keynes (1936), ao tratar sobre os motivos que levam os indivíduos a buscarem liquidez, definiu quatro fatores:

1) O motivo da renda: uma vantagem de guardar dinheiro é a possibilidade de superar o intervalo entre o recebimento da renda e o seu desembolso. A força deste motivo dependerá do nível da renda e do tempo em que o desembolso dele precisará ocorrer.
2) O motivo dos negócios: o armazenamento de dinheiro se vê pela necessidade dos empreendimentos de sobreviverem durante o período em que os custos relacionados aos negócios ainda não são sustentados pelas vendas do mesmo. Sua importância se deve à necessidade da manutenção dos fluxos de caixa em ordem.
3) O motivo precaucional: afim de poder providenciar uma solução para necessidades repentinas que exijam uma demanda de dinheiro imediata, a liquidez se torna imprescindível.
4) O motivo especulativo: um indivíduo, ao acreditar que consegue ter uma noção futura do mercado mais clara que a dos demais, se aproveita do contexto para buscar lucros. A necessidade de um mercado organizado e líquido se torna presente.

Os primeiros dois fatores podem ser incluídos no conjunto dos motivos movidos por transações e lidam diretamente no entendimento de como o comportamento humano trabalha para garantir sua sustentação.

Como dito anteriormente, Keynes focava muito na influência da incerteza no comportamento dos indivíduos. Para o autor, a solução para lidar com a incerteza era possuir ativos com alta liquidez e fazer uma boa gestão dos mesmos. Assim sendo, Keynes acreditava que o consumo, e não a poupança, garantiriam uma estabilidade maior às economias, visto que uma sociedade cujo nível de gastos se vê escassa de renda, passa a possuir resultados de desemprego maiores.

2.2.3 Keynes e a reserva de valor

Ao anunciar os postulados que viriam a definir os motivos pelos quais os indivíduos procuram liquidez, Keynes buscava entender sob qual motivação se sustentava este comportamento. Keynes (1937, p. 216) defendia sua abordagem sobre a incerteza argumentando da seguinte forma:

> ...tanto em bases racionais quanto em instintivas, nosso desejo de manter dinheiro como uma reserva de riqueza é um barômetro do nível da nossa desconfiança nos nossos próprios cálculos e convenções no que diz respeito ao futuro.

Keynes (1936) aborda o uso do dinheiro em duas vertentes: a das razões transacionais dos empreendimentos e a da reserva de valor. Embora o uso do dinheiro tenha um motivo para cada caso específico, o autor define a incerteza como uma variável de grande influência para definir como os agentes econômicos darão uso para o mesmo.

Considerando que não existam taxas de juros negativas, por que um indivíduo preferiria manter dinheiro sem gerar rendimentos ao invés de aplicá-lo em algum investimento mais lucrativo? A resposta está na incerteza que se tem a respeito das taxas de juros futuras. Se por acaso se soubesse que a taxa de juros fosse ser positiva até o vencimento do investimento, não haveria muitas dúvidas de que armazenar o dinheiro nesta condição seria a melhor saída. Logo, aqui está uma das características mais importantes da moeda para Keynes: a oportunidade de reservar valor a fim de se proteger contra incertezas.

Para Keynes (1936), outra característica necessária para que o dinheiro seja constituído como reserva de valor são seus custos logísticos ou, mais especificamente, seus custos de transação. Oautor aponta que os baixos “custos de transporte” do dinheiro jogam um papel

fundamental na manutenção deste ativo como uma reserva de valor que justifique a sua procura. Considerando que seus custos de transporte fossem grandes, o cálculo das expectativas futuras dificultaria o armazenamento do dinheiro. A capacidade dos indivíduos poderem aumentar suas reservas de dinheiro a um custo baixo, sem importar o período de armazenamento, transforma o dinheiro em um bem de alta liquidez, adequado para momentos de incerteza. Fazendo uma comparação com uma *commodity*, a dificuldade de armazenamento que a *commodity* oferece e o seu risco de desvalorização de acordo com o tempo, acabam por tornar o dinheiro em espécie um meio mais líquido e seguro.

2.2.4 White e a reserva de valor

Para White (1999), o fato de um bem como o ouro, por exemplo, possuir uma quantidade limitada, faz com que ele seja imune a variações artificiais de preço comandadas por um núcleo pensante de um Banco Central, como acontece na *fiat-money*. O preço do ouro, comandado pelo desejo dos consumidores ou pelo lucro que pode gerar a eles, pode passar a exibir um comportamento oscilante, mas fiel à vontade da maioria dos seus adeptos.

White (1999) acredita que o fato de que governos emitam dinheiro, ao mesmo tempo que realizam atos políticos a fim de manter o preço da moeda estável, não faz com que a *fiat-money* seja uma moeda na qual se pode depositar grande confiança. Para o autor, a origem e utilidade natural do ouro tornam este bem em uma boa reserva de valor, visto que possui variáveis constantes e limitadas que ajudam a delinear seu preço. Desta forma, o autor define uma *commodity* (ou "bem útil", como ele menciona) como algo que possuiria valor fora do seu contexto monetário, ou seja, um bem que é escasso e que possui demanda que não se restringe ao seu uso monetário. Ele exemplifica sua posição citando a prata, que é um bem que serve para o intuito de reservar valor, mesmo em economias onde não tenha um papel monetário. E que, a *fiat-money*, de maneira contrária, não possui utilidade fora do seu contexto monetário.

Desta forma, White (1999) define alguns critérios para considerar um bem como o ouro uma boa reserva de valor:

- Maior atratividade para contratos de longo prazo: investidores possuiríam mais interesse em fazer aplicações de longo prazo em títulos ancorados em uma *commodity* livre de intervenções estatais.
- Moeda é independente de decisões de um comitê do Banco Central: são as forças do mercado que definem o valor da moeda, e não agentes do governo, que por

variados motivos (pressões políticas e/ou ideológicas) podem vir a adulterar o preço da *fiat-money* de maneira não adequada para a sustentação do país.

- Eliminação de senhoriagem e imposto de inflação: desde que o ouro (ou moeda de estoque limitado) se mantenha com seus parâmetros de quantidade e valor inalterados, esta moeda está isenta de casos de expansão monetária ou instabilidade que faça o nível de preços aumentar.

Assim como era para Keynes, White (1999) também via o custo de utilização de um bem como uma questão pertinente à analise do valor deste bem. O ouro, por exemplo, tem um custo muito maior de produção e armazenamento do que a simples impressão de dinheiro em papel. Um país que abandonasse o modelo de *fiat-money* e adotasse uma *commodity* para usar como parâmetro de valor, passaria por choques nas contas relacionadas aos gastos decorrentes da adoção de uma *commodity* física. É questionável se a adoção de um bem que fosse mais custoso continuaria a significar que o bem serve como uma reserva de valor. Ao mesmo tempo que se poderia considerar o ouro como uma reserva de valor mais eficaz do que o armazenamento de dinheiro em papel, os custos decorrentes do armazenamento de ouro também poderiam ser maiores que os de uma *fiat-money*. Também seria necessário experimentar se a adoção do ouro como modelo único de moeda seria bem visto pela população, se ela conseguiria se adaptar de maneira confortável a este modelo.

3 A PROPOSTA

3.1 BITCOIN: A DESCENTRALIZAÇÃO DO DINHEIRO

3.1.1 O berço do Bitcoin

Embora a primeira vista, o bitcoin surja como uma proposta de moeda digital que viria a otimizar o processo de pagamentos e transferências de fundos, a característica de ser um meio de troca descentralizado o diferencia de outras experiências similares. É importante notar que, mesmo antes do bitcoin, já existiram tentativas de introduzir uma moeda digital no mercado.

Em 1998, Wei Dai, publicava seu artigo intitulado "*B-money, an Anonymous, distributed Electronic Cash System*". Com uma proposta de oferecer um canal pelo qual dois indivíduos pudessem realizar trocas sem a necessidade de um intermediário, Wei Dai anunciaria alguns dos princípios pelos quais, futuramente, o bitcoin iria se sustentar:

- Necessidade de trabalho computacional (conhecido como *Proof of Work*[3])
- Trabalho feito é verificado pela comunidade
- Transações pseudônimas entre indivíduos autenticadas através de criptografia
- Remuneração a participantes que realizassem o trabalho de verificar a veracidade das transações
- Contratos são realizados e efetuados através de assinatura digital (*public key cryptography*[4])

A proposta de Wei Dai (1998) seria o sonho anárquico de ver uma comunidade onde contratos e transferências de fundos fossem efetuados de maneira espontânea, onde a única

[3] Como explicado no artigo "Proof of Work", do site en.bitcoin.it, *Proof of Work* é um fragmento de informação com certo nível de dificuldade para ser produzido, mas fácil de ser verificado. Produzir uma *Proof of Work* tende a ser um processo demorado, que envolve processos de tentativa e erro. É através deste processo que os mineradores validam transações dentro da rede blockchain. O sistema de *Proof of Work* usado pelo protocolo do Bitcoin é o HashCash.

[4] De acordo com o site www.globalsign.com, no artigo intitulado "What is Public Key Cryptography", uma Public-key cryptography, ou criptografia assimétrica, é um sistema composto por duas chaves, a chave pública, usada para encriptar a informação, e a chave privada, usada para decriptá-la. Este sistema é aplicado em processos que buscam uma segurança efetiva quanto a privacidade de informações; diferente de um sistema simétrico de criptografia, onde a mesma chave encripta e decripta a informação, o método assimétrico dificulta o vazamento das informações. No âmbito dos negócios, pode ser usado como meio para realizar assinaturas digitais, onde o conteúdo é assinado pela chave privada e é verificado pela chave pública. O protocolo Bitcoin faz uso deste método para comprovar transações.

garantia de sucesso fosse a conduta dos indivíduos da comunidade, sem interferência de um órgão estatal. Nas palavras do próprio:

> Sou fascinado pela cripto-anarquia de Tim May. Diferente das comunidades tradicionalmente associadas com a palavra "anarquia", em uma cripto-anarquia, o governo não é apenas temporariamente destruído, mas permanentemente proibido e permanentemente desnecessário. É uma comunidade onde a ameaça de violência é impotente porque a violência é impossível, e a violência é impossível porque seus participantes não podem ser conectados a seus verdadeiros nomes ou localizações físicas.

Tim May, a quem Wei Dai se refere, se trata de Timothy May, personalidade conhecida dentro da comunidade Cypherpunk[5], da qual Wei Dai também pertencia. Timothy May ficaria conhecido pelo seu escrito de 1988 *"The Crypto Anarchist Manifesto",* uma declaração categórica contra o abuso estatal e a favor da tecnologia de criptografia digital como pilar fundamental da liberdade. Nas suas palavras:

> A tecnologia computacional está próxima de providenciar a capacidade para indivíduos e grupos se comunicarem e interagirem entre si mesmos por um método totalmente anônimo. Duas pessoas podem trocar mensagens, conduzir negócios e negociar contratos eletrônicos sem nunca terem sabido o verdadeiro nome, ou identidade, do outro... ...Reputações serão de importância central, muito mais importantes nas negociações do que os *ratings* de crédito de hoje. Estes desenvolvimentos irão alterar completamente a natureza da regulação estatal, e a capacidade de taxar e controlar interações econômicas, a capacidade de manter informações em segredo, e inclusive irá alterar a natureza da confiança e da reputação.

No mesmo ano de 1998, uma proposta alheia à de Wei Dai aparecia no cenário da criptografia, a "bit gold" de Nick Szabo. O principal foco de interesse de Szabo era a solução de problemas dentro da criptografia, em detrimento dos âmbitos de privacidade. Ao pensar na

[5] Thomas Rid (2016), em seu artigo The Cypherpunk Revolution, remete a origem do termo ao ano de 1991, quando a tecnologia de criptografia assimétrica, ou *public-key cryptography*, se difundiu ao público. Em um contexto de revolução tecnológica, detentores de computadores, munidos da tecnologia de criptografia, passaram a ser capazes de se manifestar contra o *status quo*. Em criptografia, "Cipher" é um algoritmo para encriptar ou decriptar. "Cypherpunk" surge como um trocadilho com as palavras "cipher" e "punk", uma subcultura associada com sentimentos de rebeldia.

analogia entre problemas difíceis de serem resolvidos e a dificuldade de minerar ouro, Szabo introduziu um esquema onde os responsáveis pela solução destes problemas fossem remunerados com moedas digitais. “Se um quebra-cabeças leva tempo e energia para ser resolvido, então deveria ser considerado que tem valor”, pensava Szabo.

No esquema de Szabo, um indivíduo precisaria realizar o trabalho de *proof-of-work* a fim de gerar uma solução para o problema fornecido pelo sistema. Se esta solução fosse aprovada pela comunidade, o trabalho computacional seria creditado ao autor da solução. Esta aresta do esquema viria a sustentar uma das fundações do que se tornariam as modernas criptomoedas, a remuneração para os participantes que realizassem o trabalho de verificar a veracidade das informações publicadas.

Embora fosse uma sugestão inovadora a fim de trazer indivíduos para participarem de uma comunidade descentralizada, a sugestão falhou em conseguir adeptos que confiassem na totalidade da metodologia. Uma vez que a metodologia para definir a dificuldade de um “quebra-cabeças” não era tão clara, e o sistema de remunerações era alvo de muitas dúvidas, o que passou a gerar desconfiança por parte dos programadores. Isso, aliado ao fato da dificuldade do público em designar um real valor para a moeda produzida, acabou fazendo do *bit gold* uma ideia digna de estudo, mas sem real viabilidade prática.

3.1.2 A introdução da *Blockchain*

Muito da resistência existente em relação às ideias anteriores de moedas digitais se baseava na descrença dos usuários na descentralização do sistema. Com o advento da tecnologia *blockchain*, a ideia de uma moeda digital descentralizada passaria a fazer sentido no âmbito prático. É sob este contexto, que o bitcoin surge, de maneira que sem esta tecnologia, a moeda perderia seu viés independente, tornando impossível sua execução.

Na definição de Swan (2015, p. 1) a *blockchain* pode ser conceituada da seguinte maneira:

> A *blockchain* é o livro-razão transparente e descentralizado com os registros de transações, o banco de dados que é compartilhado por todos os *nodes*, atualizado pelos mineradores, monitorado por todos e possuído por ninguém. É como uma gigante e interativa planilha que todos possuem acesso e que se atualiza e verifica que as transações digitais de fundos são únicas.

Como será visto mais a frente nesta monografia, a capacidade de verificar as transações e exibi-las públicamente para a comunidade, fez com que se resolvesse o problema das moedas

digitais anteriores, onde a cópia do ativo era infinita, impossibilitando de saber se tal quantidade de moeda já havia sido gasta antes, gerando o problema do *double-spending*. Uma vez que a *blockchain* explicita as informações da transação ao público, o risco de fraude é diminuído, já que o primeiro indivíduo que procurar fazer um ataque prejudicial ao sistema será identificado e possivelmente marginalizado da comunidade.

No entanto, mesmo que seu uso de maior nome atualmente esteja atrelado ao bitcoin, a utilização da *blockchain* transgride os limites do sistema financeiro, adentrando, inclusive, no sistema jurídico. Como apontado por Swan (2015), o ponto-chave da tecnologia *blockchain*, sua característica transparente, poderia fazer com que a tecnologia fosse usada para a realização de registro, confirmação e transferência de todo tipo de contrato. A propriedade descentralizada da tecnologia *blockchain* permite que todo tipo de registro, desde o agendamento de um quarto de hotel até a patente de uma invenção, por exemplo, possa ser visualizada e conferida de maneira fiel e simplificada.

Embora o objetivo desta monografia não seja definir os conceitos dos protocolos da *blockchain* ou do bitcoin, é impossível negligenciar como a adaptabilidade da tecnologia permitiu a criação da moeda digital de maior nome na atualidade. A inovação que a *blockchain* traz ao mercado de transferências de fundos coloca em cheque a real eficiência dos métodos convencionais do sistema financeiro e, além disso, almeja voos maiores, que compreendam uma importante parcela das atividades cotidianas dos cidadãos.

3.1.3 O anúncio

Antecedido pelo "bit gold" e sua capacidade inovadora em introduzir o conceito de *proof-of-work* para trazer soluções à tecnologia; em 2008, um indivíduo ou entidade pseudodenominada Satoshi Nakamoto[6], publicava o *white paper*[7] sobre o que viria a se tornar a criptomoeda de maior fama dos últimos tempos, o Bitcoin.

[6] Desde a época da publicação do artigo da proposta do bitcoin até o dia 4 de Outubro de 2017, a real identidade do autor tem sido mantida em sigilo. Desde 2012, o perfil de usuário de Satoshi Nakamoto no site P2P Foundation, atesta que ele possui 37 anos e reside no Japão, porém o uso perfeito da língua inglesa e o fato do software do bitcoin não ser documentado em japonês têm sugerido que ele não é japonês. Alguns indivíduos envolvidos no campo da criptografia, como Hal Finney e o próprio Nick Szabos, já foram apontados como possíveis responsáveis pela proposta, porém ambos negaram a acusação.

[7] Segundo o Cambridge Dictionary, "white paper" é um relatório do governo sobre um determinado tema, fornecendo informações e detalhes a respeito de políticas futuras. No contexto das criptomoedas, "white paper" é o documento que formaliza a proposta da moeda, explicando suas metodologias, características gerais, motivos e objetivos.

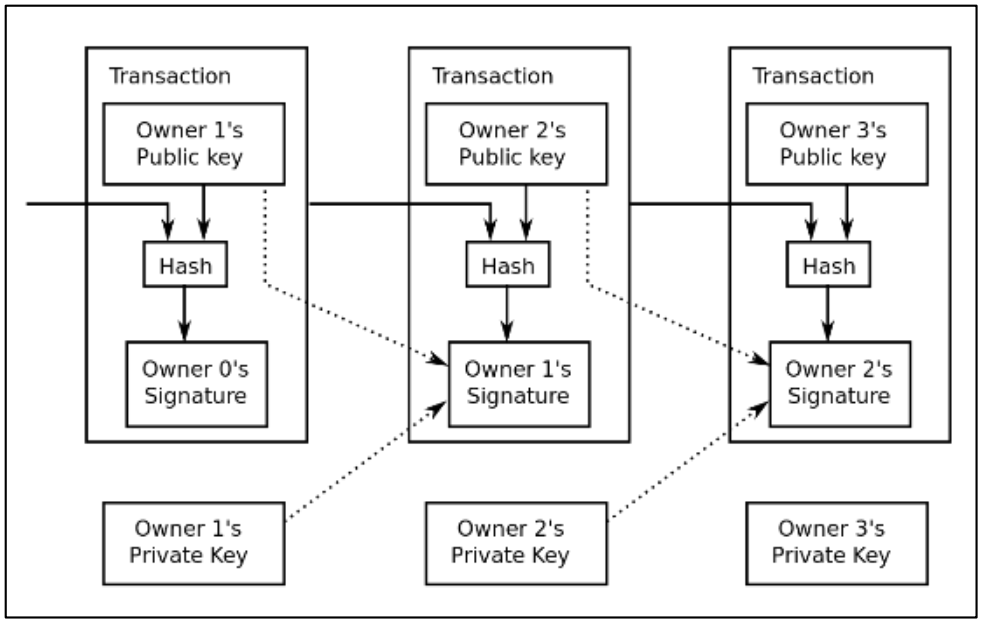
Nakamoto (2008) analisa o contexto no qual o comércio eletrônico se encontra, dando ênfase aos entraves que a necessidade de um intermediário financeiro causa aos sistemas de pagamentos e buscando oferecer uma solução para o problema do *double-spending*[8], um problema que o bit gold tinha buscado resolver anteriormente. Assumindo uma postura de rebeldia contra as instituições financeiras tradicionais, Satoshi Nakamoto argumenta que a necessidade do mercado está em um meio de pagamentos respaldado pela criptografia, e não pela mera confiança dos indivíduos entre si.

Para corrigir o problema do *double-spending*, seria necessário que houvesse um sistema que garantisse que apenas a primeira transação fosse verificada como a verdadeira, tornando inválida qualquer uma que chegasse após ela, mesmo que com a mesma assinatura digital. No entanto, um dos maiores desafios da proposta era como resolver a conciliação de transferências de fundos sem a necessidade da fiscalização de um agente de autoridade central, como um banco por exemplo. Logo, seria necessário que um sistema independente de um agente fiscalizador, fosse capaz de gerir os comandos das transferências. O primeiro esboço da proposta de Satoshi Nakamoto para resolver este problema, foi submeter as transferências à obrigatoriedade de serem anunciadas publicamente para que, desta forma, os participantes da comunidade pudessem comprovar quem realmente foi o primeiro a realizar a transferência. Para isto, seria usado o que seria denominado como *timestamp*, um servidor que iria marcar e verificar que tal conjunto de dados foi realizado em tal tempo.

Na figura a seguir, o proprietário da *public-key* número 1, ou seja, o recebedor da transferência verifica que a assinatura do proprietário número 0, o indivíduo anterior à cadeia, é verídica e condiz com o que foi acordado. Proprietário número 1 gera uma *private-key*, que servirá de assinatura para verificar a transação do proprietário da *public-key* número 2, que realiza o mesmo processo de verificação com o proprietário 1 e assim por diante.

[8] Segundo o site www.investopedia.com, o conceito de "double-spending" pode ser definido como o risco de que um gasto seja feito duas vezes, um problema exclusivo das moedas digitais, visto que informação digital pode ser reproduzida de maneira relativamente fácil e que moedas físicas não podem ser replicadas tão fácilmente, além do fato de que os agentes envolvidos em uma transação física estão habilitados para verificar, de maneira imediata, a correta transferência do valor.

Figura 1: Processo de verificação de transação no bitcoin



Fonte: Nakamoto, 2013.

Afim de implementar um sistema que pudesse marcar o tempo das transações em um contexto *peer-to-peer*, seria necessário o uso de um sistema de *proof-of-work*, o que leva o artigo de Satoshi Nakamoto de volta às ideias primordiais de Wei Dai. Para fazer o sistema funcionar, os blocos teriam que ser decifrados pelo *proof-of-work* que se encaixasse ao que cada bloco exige para liberar a informação, formando uma série de blocos em cadeia. Isto ajudaria a garantir a segurança das informações, visto que, caso um intruso quisesse alterar a informação de um bloco, precisaria fazer o trabalho computacional de todos os blocos da sequência, o que seria custoso. Logo, conforme mais blocos são conectados mais difícil é alterar a informação de um bloco passado.

Satoshi Nakamoto ordena, assim, a rede pela qual funcionaria o Bitcoin:.

1) Novas transações são transmitidas para todos os *nodes*[9].

[9] Como o site https://en.bitcoin.it/ explica, um *node* é qualquer computador que se conecte à rede Bitcoin. Os *nodes* são os elos da cadeia que verificam que as transações foram bem realizadas pelas *mining pools*, evitando problemas como o *double-spending*, por exemplo. Quando um *node* verifica uma transação ou bloco como inválidos, a ação destes é automaticamente rejeitada, mesmo que outro node considere ela como válida. Os *nodes* são responsáveis por realizar um trabalho afim de evitar que uma *mining pool* realize ataques malignos ao protocolo, impossibilitando ela de comprometer o funcionamento do sistema. Como discutido no artigo *"What are Bitcoin Nodes and Why Do We Need Them?",* do site www.coindesk.com, a ausência de incentivos para que os indivíduos realizem esforços para manter a quantidade de *nodes* ativa tem gerado preocupações em relação à segurança das transações da rede. Embora a operação dos *nodes* exija um esforço computacional relativamente similar ao das *mining pools*, a remuneração para os *nodes* é nula, tendo como única vantagem a manutenção da saúde para o sistema.

2) Cada *node* coleta novas transações dentro de um bloco.

3) Cada *node* trabalha para encontrar uma *proof-of-work* difícil para seu bloco.

4) Quando um *node* encontra um *proof-of-work*, ele transmite o bloco para todos os *nodes*.

5) *Nodes* aceitam o bloco apenas se todas as transações dentro dele são válidas e não já gastas.

6) *Nodes* expressam a sua aceitação do bloco ao trabalharem para criar o novo bloco da cadeia, utilizando o *hash*[10] do bloco aceito como o *hash* prévio.

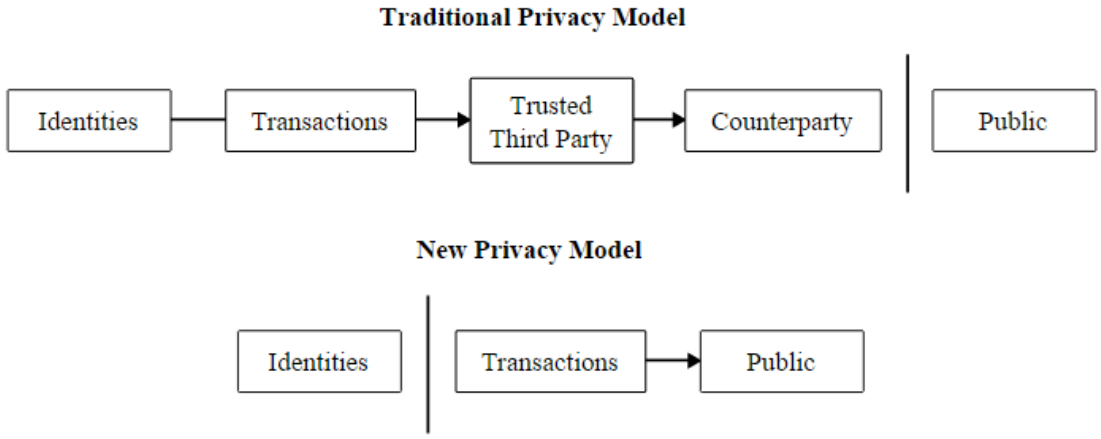
O incentivo para que os *nodes* realizem o trabalho computacional necessário para verificar as transações se sustenta na remuneração direta que o sistema fornece em troca deste trabalho. A correta construção de um bloco geraria moedas para o responsável, tornando interessante a realização do trabalho, uma vez que este mesmo pareça confiante a respeito do valor que a moeda tem. Este incentivo ajudaria os *nodes* a se manterem honestos, já que ser fiel à comunidade traria uma remuneração periódica. Realizar um ataque a alguma cadeia de blocos em busca de assaltar dinheiro não seria conveniente, visto que a própria natureza pública da tecnologia *blockchain* evidenciaria este agente como maligno, fazendo com que fosse marginalizado da comunidade.

Embora o contexto da *blockchain* seja o de manter todos os registros de transações de maneira pública, Satoshi Nakamoto, como bom discípulo de Wei Dai que era, possuía uma preocupação em garantir com que a privacidade dos usuários se mantivesse intacta ao realizarem as operações. Desta forma, diferente do modelo convencional de transações, onde a transação é identificada, processada por um intermediário de confiança e omitida do público; as transações de bitcoin sofreriam uma quebra nesta cadeia de informação, onde a identidade do agente responsável pela transação não fosse divulgada, mas que a transação em si fosse disponibilizada ao público, como demonstra o fluxograma a seguir:

---

[10] Sudhir Khatwani, em artigo intitulado *"What is a Bitcoin Hash?"* para o site www.coinsutra.com, define um algoritmo *hash* como uma função que absorve uma informação de tamanho arbitrário e a converte em uma corda de informação alfanumérica e fixa. O resultado, já ajustado ao seu tamanho fixo, é denominado de *has*h. Na rede *blockchain* do Bitcoin, o algoritmo de *proof-of-work* utilizado é baseado no SHA-256, um algoritmo de *hash* desenvolvido pela NSA (National Security Agency), em 2001. Os mineradores verificam as *hashes* em uma base aleatória e, para minerar um bloco com sucesso, os mineradores devem transformar o *hash* de um bloco em uma sequência alfanumérica. As chances de conseguir atingir este "alvo" alfanumérico específico são baixas, o que exige um processo de tentativa e erro extenso, assim justificando a necessidade de um extensivo trabalho computacional, chamado de *proof-of-work*. O primeiro minerador que encontrar a solução para o problema receberá a remuneração devida.

Figura 2: Comparativo entre o sistema de privacidade de transações tradicional e o sistema de privacidade de transações do bitcoin



Fonte: Nakamoto, 2008.

3.2 O VALOR DE UMA CRIPTOMOEDA

Dos principais receios que têm se reportado quanto às criptomoedas, talvez o maior deles seja o da instabilidade, ou falando de maneira mais detalhada, da ausência de uma proposta baseada em suficiente segurança afim de espantar a desconfiança de que as criptomoedas sejam apenas mais uma bolha financeira.

White (2014) define uma bolha como o momento em que o valor de mercado de um bem é determinado apenas pelas expectativas futuras de seu valor; sem uma base concreta que possa justificar seu interesse. Lánský (2016), ao analisar 1278 criptomoedas no período de 2013 a 2016, provou que apenas uma pequena parcela se demonstrou consistente e relativamente duradoura. A Tabela 1, a seguir, evidencia a questão da pouca durabilidade da maioria das criptomoedas. SEMANAS indica por quanto tempo a criptomoeda está ou ficou em funcionamento. TODAS indica a soma das moedas EXTINTAS e ATIVAS.

Tabela 1: Tempo de vida das criptomoedas

SEMANAS	TODAS	EXTINTAS	ATIVAS
150-174	24	1	23
125-149	43	2	41
100-124	128	21	107
75-99	139	49	90
50-74	169	84	85
25-49	234	132	102
1-25	541	399	142

Fonte: Lánský, com dados obtidos do Coinmarketcap (2015)

White (2014) comenta que, embora o surgimento de várias criptomoedas sem grande respaldo haja ocasionado bolhas no mercado, isto não significa que todas as moedas sigam um mesmo padrão, e sim que as moedas que sofreram as quedas abruptas não tinham respaldo concreto e não possuíam utilidade além do preço e sua volatilidade. O autor comenta que não é possível desconhecer que as criptomoedas que vêm obtendo maior estabilidade não tenham fundamento para respaldá-las.

Embora o respaldo técnico seja de suma importância, e que será visto mais adiante nesta monografia, White (2014, p. 14) atenta para o fenômeno da demanda por afinidade:

> Como Robert Murphy (2013) e George Selgin (2014), vários economistas propuseram que possuir Bitcoin (ou outra criptomoeda) pode providenciar uma espécie de prazer real para, ao menos, alguns dos seus detentores, como, por exemplo, anti-estatistas que gostem da moeda pelo que ela representa, entusiastas de tecnologia que admirem sua capacidade inovativa, ou seus próprios desenvolvedores que, com prazer, apostam suas próprias riquezas afim de que seus projetos sejam bem sucedidos (Luther 2013; Murphy 2013; Selgin 2014)... ...Isto não explica variações diárias no preço de mercado do Bitcoin, mas ajuda a explicar o porquê do preço estar acima de zero.

Isto também poderia explicar o sucesso da estabilidade do bitcoin em relação às criptomoedas alternativas. Por possuir o caráter inovador, todas as moedas digitais concorrentes procuram oferecer algo específico que o bitcoin não tenha. Neste processo de *catch-up* das moedas concorrentes, elas não estão imunes a oscilações de preços, visto que variações no preço do bitcoin tendem a provocar espasmos em grande parte do mercado de criptomoedas.

Da mesma forma, uma criptomoeda que não apresente real inovação aos olhos dos consumidores, possui uma tendência maior à instabilidade, como foi o caso da ZCash. No dia 28 de Outubro de 2016, a criptomoeda ZCash foi introduzida no mercado. Sua premissa consistia em reforçar a questão da anonimato, permitindo uma "divulgação seletiva" das informações contidas nas transações por cada indivíduo. Um usuário de nome "dnaleor" ao escrever o artigo *"On Fungibility, Bitcoin, Monero and why ZCash Is a Bad Ideia"* no site www.steemit.com, aponta falhas no protocolo da ZCash, como as limitações de anonimato que o sistema oferece, visto que a transação do indivíduo A apenas se manteria de maneira anônima se o indivíduo B, com quem está realizando uma transação, também adotasse o mesmo padrão de anonimato do indivíduo A. A criptografia complexa do sistema também gerou incerteza, já que as limitações e capacidades do protocolo não são tão claras. As promessas de incremento no nível de anonimato criaram uma expectativa grande em relação à moeda no momento de seu lançamento de mercado; no dia seguinte ao seu lançamento, 29 de Outubro de 2016, a unidade da moeda estava cotada a US$4293,37. Um mês depois, 29 de Novembro, a moeda estava precificada a US$69,09. A moeda se manteve neste patamar até Maio de 2017, onde atingiu os US$257,27, sem sofrer grandes alterações até Setembro do mesmo ano, quando estava cotada a US$219,42.

Van Alstyne (2014), no artigo *"Why Bitcoin Has Value"*, lista três argumentos para a valorização do bitcoin:

- Transparência: o bitcoin, por estar inserido no sistema *blockchain*, fornece um registro público de transações. Desta maneira, o risco de pagamentos duplicados é diminuído em grande escala. Toda transação possui um comprador, um vendedor, e um montante, que pode ser fiscalizado por qualquer indivíduo com acesso a internet.
- Comércio sem amarras: as baixas taxas de transação incentivam o desenvolvimento da economia. Empresas de cartões de crédito, adquirentes de crédito e operadores de câmbio, podem chegar a cobrar quantias consideráveis de taxas para a realização de transações. Isto desestimula os comerciantes a oferecerem meios de pagamentos que poderiam engrandecer os negócios.
- Aceitação da Comunidade: bitcoin não é uma moeda imposta como regra para a realização de pagamentos e transferências de fundos. Sua valorização vêm por atender os requisitos para algo se tornar "dinheiro", visto que é um meio de troca, possui reserva de valor e é uma unidade de conta.

Embora, à época de publicação do artigo, as taxas de transação do bitcoin fossem consideravelmente baixas, isso não é mais algo tão indiscutível no tempo presente. O alto nível de movimentação e de demanda por bitcoins têm provocado mudanças na estrutura de transferências da moeda. Mais adiante na monografia, isto será tratado em uma seção específica.

Quanto ao bitcoin se caracterizar como "dinheiro", há opiniões que contrastam esta posição. Yermack (2013) argumenta que a alta oscilação do bitcoin impede esta mesma de atender o requisito de ser uma unidade de conta. Para o autor, esta mesma volatilidade afeta diretamente os anseios do bitcoin como reserva de valor. A dificuldade de correlacionar o bitcoin com as principais moedas do mundo tornaria o bitcoin imune a impactos macroeconômicos na economia global. Para o autor, os dados mostram que um bem que se distancia dos comportamentos das grandes moedas globais não serve como meio de *hedging* ou como utensílio para estratégias de *risk management*, assim diminuindo a utilidade do bitcoin. Ao correlacionar a influência do bitcoin nas moedas de grande impacto global, o autor sustenta sua tese, mostrando o bitcoin como uma moeda completamente imprevisível, assim demonstrando a dificuldade em elevar a criptomoeda ao patamar de moeda global. Na Tabela 2 a seguir, matriz de correlação de mudanças diárias nas taxas de câmbio no bitcoin e no ouro. A tabela mostra simples correlações das mudanças percentuais em taxas de câmbio diárias para pares de moedas, com todas as taxas de câmbio medidas contra o dólar americano:

Tabela 2: Matriz de correlação EUR x JPY x CHF x GBP x Ouro x Bitcoin (19/07/2010-29/11/2013)

	EUR	**JPY**	**CHF**	**GBP**	**Ouro**	**Bitcoin**
EUR	1.00	0.19	0.60	0.65	0.21	0.05
JPY		1.00	0.33	0.21	0.08	-0.02
CHF			1.00	0.42	0.20	0.04
GBP				1.00	0.21	0.02
Ouro					1.00	0.06
Bitcoin						1.00

Fonte: Yermack, 2013.

Ulrich (2014) admite a dificuldade de adotar o bitcoin como unidade de conta enquanto a volatilidade continuar se manifestando como algo característico. Porém, argumenta que o processo de aumento de liquidez e de aceitação poderia vir a tornar o bitcoin um utensílio indispensável para o cálculo econômico, onde produtos e serviços sejam precificados em função da moeda. O autor equipara o bitcoin ao ouro e à prata, elevando o bem ao posto de "moeda natural", onde sua origem se fundamenta nos anseios espontâneos dos indivíduos. Esta cooperação voluntária não apenas permitiria como auxiliaria o bitcoin a se tornar, além de um meio de troca e reserva de valor, uma unidade de conta.

Desde o *b-money* de Wei Dai até a atualidade, nenhum projeto de moeda digital surgiu com tanta força quanto o bitcoin. Muito do que existe no bitcoin foi derivado de projetos anteriores, como o próprio *b-money*, porém, não se deve negligenciar a originalidade do protocolo de Satoshi Nakamoto e, embora diagnosticar a moeda como uma certeza ainda seja entrar no campo da especulação, é interessante evidenciar a importância da volta da moeda digital como um movimento renovado, capaz de atrair não somente apoiadores dentro do âmbito *mainstream*, mas também a suspeita e até crítica de setores que costumavam ignorar estes projetos no passado, como os grandes bancos, por exemplo.

4 VIABILIDADE

4.1 DESCENTRALIZAÇÃO DA MOEDA

Para os defensores das criptomoedas, um dos grandes atributos da tecnologia é sua capacidade descentralizadora. A habilidade de poder realizar pagamentos e transferências sem intermediários facilitaria acordos entre os indivíduos e reduziria a burocracia dos processos inerentes ao modelo tradicional de transferências, como o método SWIFT, por exemplo..

Para analistas mais inconformados com o monopólio do dinheiro oferecido pelo Estado, a natureza descentralizadora do bitcoin providencia uma opção alternativa, que confronta diretamente os anseios dos governos. Ulrich (2014) aponta que o bitcoin pode vir a se manifestar como uma ferramenta de combate aos regimes intervencionistas estatais, anunciando a chegada da tecnologia como um ponto de inflexão na história monetária mundial.

O aspecto descentralizador do bitcoin faz com que não haja um órgão máximo que regule os fluxos da moeda. Por possuir um protocolo programado afim de não ultrapassar a liberação de 21 milhões de bitcoins, a proposta da moeda indica que, diferente dos Bancos Centrais, o sucesso ou insucesso do bitcoin será guiado pela livre iniciativa de seus usuários e pela viabilidade que a moeda terá no núcleo das sociedades.

Como apontado por Van Alstyne (2014), analistas do Federal Reserve Bank se manifestaram receosos em relação à adoção do bitcoin, justamente porque a ausência de um grupo central capaz de definir os rumos da moeda, poderia gerar ao menos dois problemas: volatilidade e reserva de valor arriscada. Para o autor, isto não inviabiliza a moeda, apenas a torna pouco atrativa para indivíduos avessos ao risco. Em outras palavras, se a tecnologia realmente se demonstrar robusta, e passar confiança para seus usuários, é menos provável que um único indivíduo possa realizar choques de preço ou ataques especulativos na moeda.

Na prática, a proposição de Van Alstyne, que diz que a volatilidade não afetaria a viabilidade da moeda, tem se mostrado, pelo menos, confusa. Embora a popularização da moeda tenha sim aumentado e passado a fazer parte do cotidiano em um ritmo mais agressivo, determinados eventos têm afetado a estabilidade da moeda.

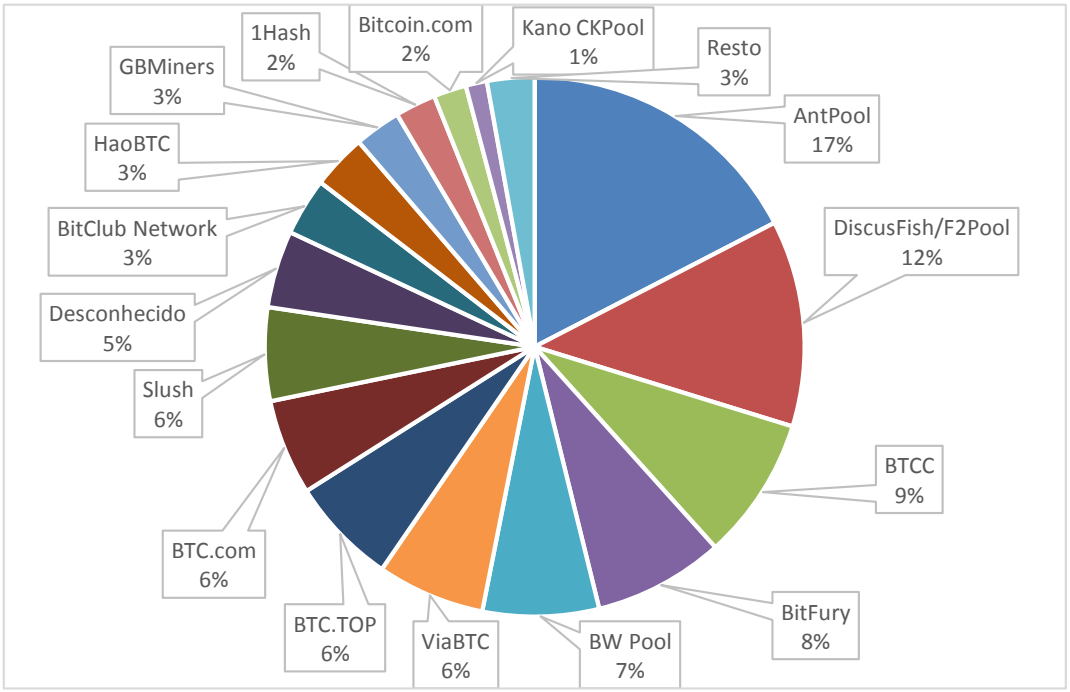
No dia 4 de Setembro de 2017, o Banco Central chinês decidiu que passaria a proibir as ICOs[11], alegando que estas vendas violavam a lei chinesa e deveriam ser paradas imediatamente. Uma semana antes da decisão, o preço do bitcoin estava cotado próximo aos US$5.000,00. Na manhã seguinte à intervenção chinesa, o preço declinou para os US$4.300. Estes movimentos levam a crer que a volatilidade do bitcoin leva em conta uma quantidade maior de fatores, e que a mera popularização da moeda não tem se mostrado capaz de, por si só, transformar o bitcoin em uma moeda estável.

Embora a proposta do bitcoin se sustentasse no alicerce da descentralização total dos processos, incidentes recentes têm colocado pontos de interrogação quanto a isto. Uma ameaça à ideia de descentralização estaria em justamente uma das entidades da cadeia responsável pela distribuição dos bitcoins: os mineradores.

Afim de garantir a remuneração aos mineradores, o processo de programação feito por estes mesmos é administrado por uma *mining pool*; uma espécie de administradora de mineradores. Esta administradora computa todos os problemas a serem resolvidos pelos mineradores para que uma transação seja bem sucedida, assim a *mining pool* identifica o problema e repassa o trabalho para os participantes. Com uma estimativa de dados entre Setembro de 2016 e Setembro de 2017, é possível ter uma noção da distribuição de mercado dos *mining pools*, como apresentado pela Figura 3 a seguir:

[11] Como explicado pelo site www.bitcoinmagazine.com, uma ICO (Initial Coin Offeriing), é um mecanismo de levantamento de dinheiro para financiar projetos envolvendo criptomoedas, onde os proponentes dos projetos aceitam dinheiro dos investidores, e em troca entregam participação no projeto. A semelhança com a IPO se dá por conta da relação entre investidor e projeto. Embora as ICOs tenham aparecido recentemente, já foram vítimas de diversas controvérsias, sofrendo acusações de serem um esquema inseguro e desregulado de levantar dinheiro. A SEC (U.S. Securities and Exchange Commission), órgão responsável pela fiscalização dos valores mobiliários americanos, soltou uma nota no dia 25 de Julho de 2017, manifestando uma posição que evidencia que passará a tratar as atividades das ICOs como valores mobiliários e que, portanto, estarão sujeitas às regulações vigentes.

Figura 3: Distribuição do mercado de *mining pools*, por taxa de *hash*



Fonte: Elaboração própria, dados angariados no site www.blocktrail.com

Como apresentado na Figura 3, 53% da taxa de *hash*, ou seja, produção do bloco do bitcoin, está concentrada em apenas 5 mining pools: AntPool, Discusfish/F2Pool, BTCC, Bitfury e BW Pool. Em um cenário onde houvesse a formação de um conluio entre estas 5 *mining pools*, a possibilidade de danos ao protocolo poderia ser, ao menos, debatida.

Gervais *et al* (2014), chega a colocar uma situação hipotética, onde a formação de um conluio de *mining pools*, que possuísse parcela de mercado maior a 50%, poderia vir a se tornar uma ameaça à proposta original, visto que estas mesmas teriam capacidade de controlar a confirmação de todas as transações do sistema. Isto poderia fazer com que determinadas transações fossem proibidas de serem executadas, ou com que transações suspeitas fossem aprovadas sem um critério aprovado pela comunidade inteira.

Diante desta ameaça, começaram a surgir projetos de *mining pools* descentralizados. Estas *mining pools* independentes compartilhariam os mesmos benefícios das *mining pools* convencionais, apenas sem um controle central. Até a data de 08 de Setembro de 2017, a mineradora independente com maior parcela de mercado é a P2Pool, com 0,16% de criação de blocos entre Setembro de 2016 e 2017. Como o próprio nome sugere, a mineradora funciona através de um protocolo *peer-to-peer*, onde não há um único servidor central. A iniciativa de tentar evitar a degradação do sistema descentralizado do bitcoin tem feito com que entusiastas

da concepção original da tecnologia mantenham o funcionamento da P2Pool através de doações.

4.2 RISCOS E SEGURANÇA

Murdoch e Anderson (2014) discutem alguns impedimentos para a atuação das criptomoedas, mais especificamente o bitcoin, como moeda alternativa para o dinheiro emitido pelo Estado. Para os autores, o bitcoin ainda poderia ser alvo de coerção das autoridades, visto que as grandes casas de câmbio, detentoras de grande porcentagem dos bitcoins emitidos, não possuem anonimato. Isto significaria que, uma vez que as autoridades identifiquem algum fluxo de bitcoins como suspeito, poderiam pressionar as casas de câmbio para que "congelassem" estes bitcoins.

Outra questão apontada pelos autores, é a que a emissão de novos bitcoins está centralizada em muito poucas mineradoras. Ou seja, embora uma vez emitido o bitcoin, este seja descentralizado, a origem destas moedas foi viabilizada por um seleto e diminuto grupo de pessoas que, da mesma maneira com que acontece com as casas de câmbio, poderia ser vítima de pressões de autoridades, quando estas não concordassem com tais atividades. Da mesma maneira, mineradoras que fossem vítimas destas pressões e tivessem que cessar a operação, passariam a deixar uma fatia maior de mercado para os mineradores restantes. Isto poderia vir a gerar uma desconfiança na moeda e gerar dúvidas a respeito da independência do sistema.

Os autores apontam para outra fragilidade do sistema, ao definirem que a falta de um órgão máximo que represente e emita os bitcoins viria a aumentar o risco de crédito por parte dos detentores da moeda. Justamente pela premissa do bitcoin ser a de representar uma moeda independente do controle estatal, os adeptos da moeda não possuiriam um fundo garantidor de crédito, em caso de perdas, roubos, ou até mesmo o esquecimento da senha de acesso à carteira virtual de bitcoins. Embora esses riscos sejam, sim, plausíveis e de fato, já tenham acontecido[12], existem métodos de segurança que se contrapõem ao argumento dos riscos mencionados. Como

[12] No dia 7 fevereiro de 2014, Mt. Gox, a casa de câmbio de bitcoins com maior volume e número de transações à época, suspendeu todas as retiradas de bitcoin do seu *website*, alegando problemas técnicos e a realização de manutenção. No dia 24 de Fevereiro do mesmo ano, o *website* suspendeu todas as operações de *trading*, e horas depois, o *website* saiu do ar. Um documento interno vazado indicou que a empresa estava insolvente, após a perda de 744.408 bitcoins. Em 28 de Fevereiro, a companhia anunciou que perdera quase 750.000 bitcoins de clientes e 100.000 próprios. No dia 20 de Março, a empresa anunciou que encontrara 200.000 bitcoins em uma *digital wallet*, trazendo a perda total para 650.000.

Blundel-Wignall (2014) aponta, segurança adicional contra ataques de *hackers* pode ser providenciada pelo uso de um utensílio de *cold storage*, ou seja, o armazenamento de moedas digitais em meios físicos.

Teo (2014, p. 4), comenta:

> Assim como você pode perder seu dinheiro, você pode perder seus bitcoins. Se você não faz um back-up da sua carteira digital guardada no telefone celular, por exemplo, você perderá seus bitcoins quando perder seu telefone celular. Se você guarda suas moedas encriptadas no seu computador, e *hackers* invadem seu computador tais quais ladrões invadem sua casa, você perderá seus bitcoins. Alguns usuários recorrem ao *cold storage* para proteger seus bitcoins. *Cold storage* significa armazenar seus bitcoins de maneira off-line. Você pode imprimir seu código bitcoin em um pedaço de papel e trancá-lo num cofre. Você também poderia armazenar suas moedas em um disco USB ou disco rígido, desconectá-lo do computador e guardá-lo onde quiser. No entanto, se você perder o papel ou o disco, você também perderá seus bitcoins.

Esta noção busca desmistificar a ideia de complexidade do risco de uma criptomoeda e colocá-las ao mesmo nível do dinheiro corrente utilizado. Diferente do dinheiro físico, com o bitcoin o indivíduo teria várias possibilidades de *back-ups*. A resistência que o bitcoin encontra para ser reconhecido como uma moeda genuína também gira em torno de se tratar de um ativo quebrador de barreiras, um ativo diferente do usual; uma resistência similar à que a Internet sofreu. Da mesma forma, negligenciar o potencial do bitcoin pode vir a se tornar uma posição equivocada, como McCallum (2015, p. 354):

> Pode ser questionado como alguém poderia, racionalmente, considerar algo que não a probabilidade de uma resistência governamental ao bitcoin. Para mim, no entanto, parece improvável que o bitcoin substitua as moedas estatais em larga escala. Porém, se eu pensar de volta no começo dos anos 1990, eu mesmo nunca teria acreditado que o e-mail e a Internet teriam tantas proporções ao ponto de tomarem uma grande parte das minhas atividades diárias como, de fato, elas tomaram.

Para o autor, embora uma ameaça do Federal Reserve Bank à prosperidade do bitcoin seja uma possibilidade digna de ser levada em conta, a natureza jurídica dos Estados Unidos fornece certa proteção ao livre movimento de moedas no país, visto que a constituição americana não diz nada a respeito de companhias privadas criando dinheiro (GRINBERG, 2011).

4.3 CONFRONTO COM A TEORIA

Como explicitado anteriormente, um importante pilar da teoria keynesiana da moeda se sustentava na preferência por liquidez. Quando se coloca a história do comportamento do bitcoin contra a teoria keynesiana, algumas contradições surgem. O fato do bitcoin ter se demonstrado como uma moeda de preço instável ao longo de sua curta trajetória, coloca em xeque os anseios dos seus criadores e apoiadores de ser uma moeda capaz de reservar valor.

Elencando os quatro fatores que John Maynard Keynes caracteriza como responsáveis por fazerem os indivíduos buscarem liquidez em um ativo, o único que parece, até o momento, se adequar ao bitcoin, é o motivo da especulação. Não há duvidas de que a grande oscilação de preço do bitcoin tem atraído investidores ávidos por lucros[13], o volume crescente de transações (ver Figura 4) fala por si só. No entanto, os outros três motivos anunciados por Keynes, o da renda, o dos negócios e o precaucional, exigem que exista uma condição de pouca incerteza em cima do dinheiro. Seja para manter a saúde dos fluxos de caixa de uma empresa, seja para atender demandas emergenciais, o dinheiro deve ser de fácil retirada e de valor estável, segundo Keynes.

Assumindo a posição de White e elencando a prata como um bem que reserva valor e vai além do mero papel monetário, é possível criar uma tentativa de nexo deste bem com as criptomoedas. Para o autor, o processo que leva uma *commodity*, como o ouro ou a prata, a tomar o posto de dinheiro depende do cumprimento de quatro pressupostos:

---

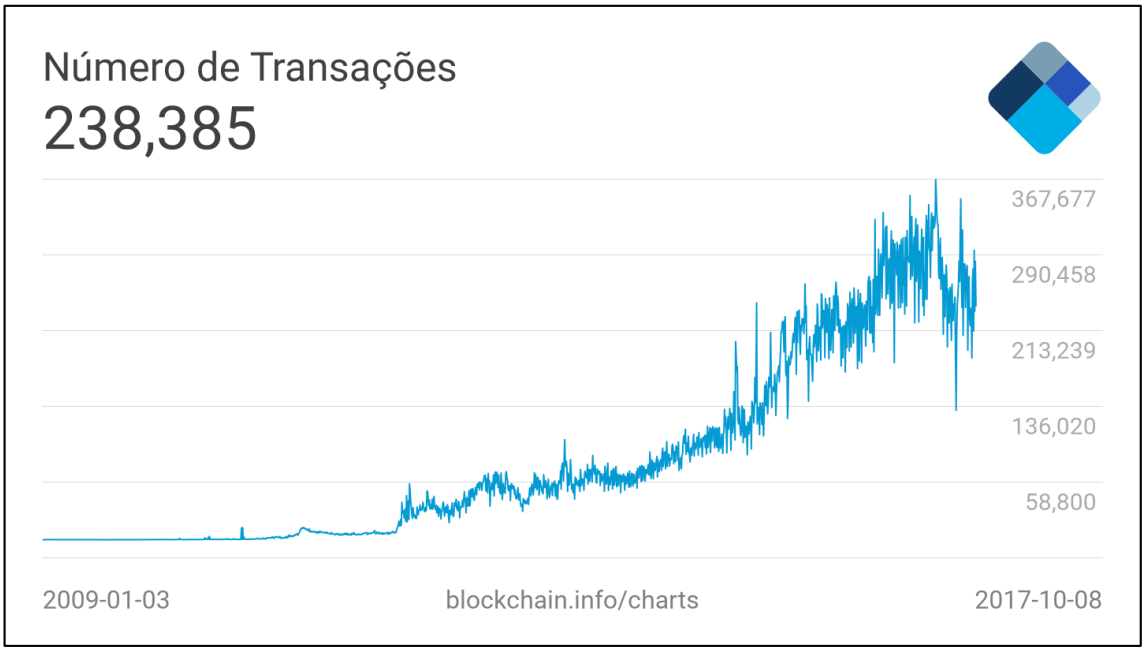
[13] No artigo *"Bitcoin Is Attracting Serious Skeptics Despite Rising Euphoria"*, publicado para o site www.thestreet.com por Tanzeel Akhtar, no dia 14 de Agosto de 2017, se discute a introdução do bitcoin como ativo de interesse nos meios mais sofisticados de investimentos. Josh Brown, CEO da Ritholtz Wealth Management fez uma publicação anunciando sua primeira compra de um bitcoin através da Coinbase, casa de câmbio americana de bitcoins. Josh diz que não é nenhum revolucionário ou *early adopter*, e sim apenas um investidor curioso demais para deixar passar esta oportunidade. Tim Courtney, CIO da Exencial Wealth Advisors, embora acredite que as criptomoedas ainda não possuam liquidez suficiente, admite que já recebeu, dos seus clientes, uma demanda grande de pedidos por informações a respeito de criptomoedas. Como informado pelo site www.cointelegraph.com, no artigo *"Australian Move to Legalize Bitcoin Attracts Gold and Bullion Investor"*, publicado por Joshua Althauser, no dia 04 de Setembro de 2017, Paul Engeman, diretor da Ainsle Bullion and Reserve Vault, firma australiana focada no comércio de ouro e prata há 43 anos, passou a receber uma alta demanda por bitcoins de novos e existentes clientes, que viram no bitcoin, um ativo com particularidades semelhantes ao ouro e prata. A eliminação de impostos na compra de moedas digitais por parte do governo australiano auxiliou ao aumento da procura pelas criptomoedas.

- Possuir uniformidade. Atestar a qualidade do ouro e da prata é muito mais simples do que a qualidade de uma folha de tabaco, por exemplo.
- Ouro e prata são bens duráveis. São resistentes ao teste do tempo.
- Bens divisíveis e fungíveis. Diferentes quantidades de pagamentos podem ser feitas dividindo o tamanho do metal.
- Vantagens logísticas. A facilidade que se tem para transportar ouro e prata valoriza estes bens. É mais fácil andar com menos peso, incorre-se em menos custos.

Para o primeiro pressuposto, o da uniformidade, ser validado, as criptomoedas precisariam ter atingido um estágio de maturidade e consistência maior, as dúvidas acerca da viabilidade destas moedas digitais a impedem de ser um ativo indiscutivelmente valioso. Para o segundo, da durabilidade, o aspecto inovador das criptomoedas as impede de serem reconhecidas como bens duráveis, sua grande volatilidade no preço também afeta esta posição. O terceiro e quarto pressupostos parecem ser atendidos de maneira eficiente até o momento, considerando que as criptomoedas são bens facilmente fracionáveis, e que permanecem sendo uma opção interessante para a realização de transferências, considerando seus baixos custos de transação.

O propósito do bitcoin vai na contramão, pelo menos até a data desta monografia, dos requisitos de Keynes, no entanto, adéqua-se, em certo nível, às ideias de White (1999), que vê uma alternativa à *fiat-money* como uma oportunidade para possuir uma reserva de valor alheia às decisões políticas estatais. Porém, fazendo as devidas ressalvas, a instabilidade do poder inovador do bitcoin acaba tornando a criptomoeda em um ativo diferente do ouro, objeto de análise de White; ou seja, mesmo que o bitcoin seja independente de forças estatais, possua um estoque limitado e esteja imune à senhoriagem, a instabilidade da criptomoeda a acaba enfraquecendo no que tange a uma moeda com reserva rígida de valor. No entanto, um dos motivos desta instabilidade pode estar na capitalização de mercado bastante inferior que o bitcoin tem em relação ao ouro, por exemplo. Enquanto a criptomoeda, no dia 15 de Novembro de 2017, possuía um volume total de moedas em circulação equivalente a US$122 bilhões, o ouro, à mesma data, contava com um valor superior aos US$7 trilhões. Isto poderia explicar a maior rigidez do ouro em relação ao bitcoin, visto que para este último, ainda existe muita margem para mudanças.

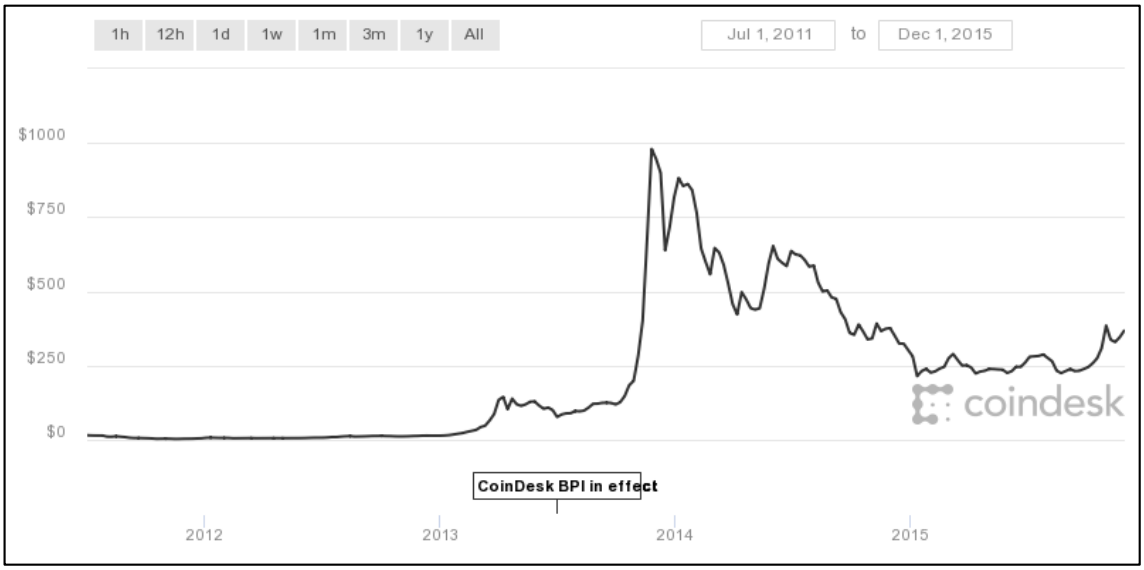
Figura 4: Acompanhamento do número de transações envolvendo bitcoin na rede *blockchain* no período entre 03/01/2009 e 08/10/2017



Fonte: Site www.blockchain.info/charts

Bouri *et al* (2016), através de uma análise econométrica que correlaciona a movimentação de preço do bitcoin com as principais bolsas mundiais no período 2011-2015, mostra que é possível ver uma valorização diária e semanal muito maior da criptomoeda em relação com a movimentação de preços das bolsas. No entanto, ao mesmo tempo em que a valorização foi maior, um nível grande de volatilidade (ver Figura 5) se mostrou presente no período analisado. Assumir uma boa valorização da moeda como suficiente para descrever o bitcoin como uma moeda estável é tomar uma postura arriscada, que não considera a criptomoeda como uma oportunidade de reserva de valor e sim como mero ativo especulativo, não atendendo todos os motivos da preferência por liquidez indicados por Keynes.

Figura 5: Acompanhamento do preço do bitcoin, em dólares americanos, entre 01/07/2011 e 01/12/2015.



Fonte: www.coindesk.com/price

Os aspectos regulatórios pelos quais o bitcoin ainda pode vir a passar funcionariam como mais um elemento de argumentação contra sua liquidez. Embora a proposta do bitcoin trate os usuários do sistema como pseudônimos, anunciando que todas as transações são públicas, paira uma preocupação quanto ao uso do sistema do bitcoin como instrumento para evasão e sonegação de impostos.

Segundo Marian (2013), o governo alemão já sugeriu taxar o bitcoin como um ativo de capital. No entanto, isto não evita que o usuário mantenha seus bitcoins em sua forma pura, sem trocá-los por uma moeda estatal, assim evitando a taxação. Isto leva a crer que as forças estatais poderiam se encontrar em uma situação onde precisariam tomar uma atitude mais agressiva contra o uso dos bitcoins, como proibir qualquer transação e/ou pagamento de criptomoedas, onde mesmo não resolvendo o problema da evasão de impostos, a credibilidade do bitcoin poderia se ver abalada, fazendo com que, indiretamente, o bitcoin deixasse de ser uma espécie de paraíso fiscal tão interessante. Embora ações como essa desestabilizariam o bitcoin e, por consequência, o tornariam menos líquido, políticas intervencionistas a esse ponto poderiam gerar uma sensação de desconforto da população que, temendo o poder excessivo do estado, passaria a desconfiar dele.

5 CRIPTOMOEDAS CONTRA O CENÁRIO ATUAL

5.1 SISTEMA SWIFT VERSUS TECNOLOGIA *BLOCKCHAIN*

Ao se falar de novas tecnologias, é importante identificar o porquê de elas estarem em voga. A chegada da tecnologia *blockchain* para os meios de pagamento não é um instrumento para realizar operações concretamente diferentes das que existem hoje, mas sim representa uma inovação ao processo, uma nova ótica para algo que já existia. Embora seja discutível a real aplicabilidade desta tecnologia neste meio, como explicado antes, seria pouco cuidadoso negligenciar este projeto, visto que tem tido consistência suficiente para chamar a atenção de agentes importantes do segmento financeiro e bancário.

Para entender como a tecnologia *blockchain* surge com tanto vigor, é necessário compreender a situação do sistema de transferências de fundos internacional e como ocorreu sua fundação. A principal referência que se tem na atualidade com relação às transferências internacionais é o que se conhece como o método S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunication), um sistema padronizado que permite às instituições financeiras realizarem suas operações de transação.

De acordo com Scott e Zachariadis (2009), as fundações do método SWIFT podem ser traçadas à década de 1840, quando os recém-introduzidos telégrafos foram capazes de realizar comunicações dentro do mercado de ações americano. Avanços posteriores acabaram por trazer o instrumento conhecido como *teleprinter exchange*, popularmente conhecido como Telex. O Telex viria a ser introduzido primeiramente na Alemanha pré-Segunda Guerra Mundial, como um aparelho que poderia mesclar a comunicação falada e digitada (BEAUCHAMP, 2008). A sua operação mais simples em relação ao telégrafo, atraiu o interesse dos bancos, que buscavam reduzir custos através de processos de automatização.

Com os bancos buscando concretizar operações globais afim de estabelecer negócios internacionais, o Telex seria a ferramenta adequada, considerando sua facilidade em aprimorar as comunicações internacionais. Embora o Telex fornecesse o caminho para facilitar as negociações internacionais, o processo de troca de informações não era uniforme e existiam diversas versões e linguagens (SCOTT, ZACHARIADIS, 2009). Isto demandou um acordo entre os bancos para a criação de uma linguagem-padrão de maneira a reduzir impasses.

No intuito de reduzir riscos operacionais entre as transferências dos bancos, era necessário manter equipes específicas para gerenciar o bom funcionamento das transações bancárias. Depois de uma série de reuniões e pesquisas conduzidas por consultores financeiros e bancos

entre 1971 e 1972, no dia 3 de Maio de 1973, a SWIFT seria fundada (SCOTT, ZACHARIADIS, 2009). Desde a década de 70, quando o sistema financeiro internacional passou a ser digitalizado, a maioria das instituições financeiras acordou em adotar o método SWIFT de transferências internacionais. Conectando mais de 11.000 instituições e 200 países, esta plataforma vem sendo utilizada desde então como o principal mecanismo de trocas de informações e ofertas de produtos e instrumentos financeiros internacionais.

Embora lide diretamente com atividades financeiras, é importante evidenciar que o sistema SWIFT, em si, não realiza as transferências de fundos, e sim funciona como um mecanismo de mensagens interligadas, onde os comandos são efetuados pelos bancos participantes. Baker e Byler (1983) definem o Sistema SWIFT como uma rede privada de comunicações, utilizando o que há de mais recente na tecnologia de telecomunicações e que é importante evidenciar o fato de que o sistema SWIFT não é um sistema de pagamentos *per se*, visto que os acordos ainda são delineados pelos bancos.

O artigo, datado de 1983, poderia definir com muita precisão o estado do sistema SWIFT nos dias contemporâneos, visto que poucas alterações foram feitas. De fato, os custos das transferências têm diminuído como dados do Banco Mundial apontam. No entanto, a tecnologia do método SWIFT parece defasada, abrindo terreno para a entrada de novas tecnologias que possibilitem, ao menos, um trabalho logístico menor do que as atuais instituições oferecem, e nisso as criptomoedas podem surgir como opção alternativa.

Segundo publicação da própria SWIFT, em 12 de Janeiro de 2017, uma grande porção dos custos das transações é destinada ao processo de verificações de débitos e créditos ao fim do dia, feitos pelas instituições financeiras. Tendo isso como contexto, a organização admitiu estar atenta aos avanços tecnológicos da área, e divulgou o lançamento de um *Proof of Concept* (PoC) destinado exclusivamente a pesquisar a viabilidade da *distributed ledger technology* (DLT), afim de otimizar os processos de transações e diminuir riscos operacionais e custos excedentes.

No entanto, a popularização da tecnologia *blockchain* não deveria necessariamente ser vista como a independência total do indivíduo para com os bancos. Conforme evidenciado em relatos recentes, grandes bancos como Goldman Sachs, JP Morgan, Santander, entre outros, já se encontram investindo em pesquisa relacionada à tecnologia. Um deles, o Credite Suisse, em relatório publicado no dia 3 de Agosto de 2016, de autoria de Charles Brennan, se mostrou favorável à adoção da tecnologia. Embora o autor comente que não acredita no bitcoin como um sistema durável de pagamentos, incapaz de se equiparar a grandes marcas como Visa e Mastercard, por exemplo, ele confia que a tecnologia descentralizada do *blockchain* é capaz de

superar as características ultrapassadas do método SWIFT. De acordo com o autor, com custos de transferência chegando até os 10% do montante total transferido no método SWIFT, uma tecnologia rápida, confiável e muito menos custosa seria de grande utilidade para os bancos e poderia vir a significar um atrativo a mais para organizações multinacionais com fluxos internacionais frequentes.

O que se entende de uma posição como esta é que se pode esperar que a tecnologia *blockchain* passe a fazer parte de projetos de inúmeros empreendimentos, até mesmo dos grandes bancos. No entanto, a concepção de uma criptomoeda como moeda real de circulação parece não fazer parte dos planos destes agentes. Como reportado no artigo "*Bitcoin is a fraud that will blow up, says JP Morgan boss*", publicado no The Guardian no dia 13 de Setembro de 2017, de autoria de Angela Monaghan, o CEO do JP Morgan, o maior banco de investimento dos Estados Unidos, Jamie Dimon, expressou todo seu descontentamento em relação à ideia do bitcoin, reduzindo a sua importância a uma mera opção para indivíduos em condições remotas:

> A moeda não vai funcionar. Você não pode ter um empreendimento onde pessoas inventem uma moeda do nada e acredite que pessoas que estão comprando ela são muito espertas. Se você estivesse na Venezuela, no Equador, na Coreia do Norte ou em lugares assim, ou se você fosse um traficante de drogas, um assassino, coisas como essa; você está melhor se virando em bitcoin do que em dólares americanos... então, talvez haja um mercado para isso, mas seria um mercado limitado... honestamente, eu apenas estou chocado que ninguém consiga ver isso pelo que é.

No dia 12 de Setembro de 2017, o preço do bitcoin fechou a US$4130,81. No dia 13 de Setembro, após Jamie Dimon fazer suas declarações, a moeda fechou o dia a US$3882,59, sendo que no dia seguinte fechou a US$3154,95, uma queda de 23,63% em relação ao preço antes das declarações. Já foi comentado nesta monografia como seria muito ingênuo conferir a volatilidade do preço do bitcoin a uma variável simples como essa, no entanto, serve para ilustrar, de certa maneira, o impacto que as instituições financeiras tradicionais podem ter sobre as criptomoedas.

5.2 NOVO MERCADO DE TRANSFERÊNCIAS DE FUNDOS

Novas modalidades de pagamento sustentadas pela tecnologia *blockchain* seriam capazes de impactar diferentes camadas da sociedade.

Um dos segmentos atingidos seria a da força de trabalho estrangeira, que envia remessas de dinheiro a seus países de origem. Segundo estimativas compiladas por Manuel Orozco, diretor do Migration, Remittance and Development Program, do *think tank* Inter-American Dialogue, o custo médio de taxas de transação para trabalhadores que enviassem US$200 para seus países de origem na América Latina, em novembro de 2002, era de US$16,02, em uma amostra de 70 empresas.

Por se tratar de um assunto que lida diretamente com imigrantes, Manuel Orozco foca muito na questão dos mexicanos residentes nos Estados Unidos. Segundo a American Community Survey de 2015, censo realizado pelo governo americano, a população mexicana residente no país era composta de 11 milhões e 643 mil pessoas, ou 26,9% de toda a população imigrante do país. Segundo estimativas do Banco Mundial do primeiro trimestre de 2017, o custo médio de transação de uma remessa de US$200 originada nos Estados Unidos com destino ao México, era de US$9,33, ou 4,67% do valor bruto da transação. Esta simulação toma em consideração 26 modalidades de transferência de dinheiro, distribuídas em 11 instituições. Levando essa simulação para o primeiro trimestre de 2011, desta vez considerando 20 modalidades de transferência e 14 instituições, o custo médio de transação para a mesma remessa de US$200 era de US$10,96, ou 5,48% do valor bruto da transação.

A seguir, a Tabela 3 apresenta características médias de transferências no primeiro e terceiro semestre do período compreendido entre 2009 e 2017:

Tabela 3: Custo de transação de uma remessa de US$200,00 dos Estados Unidos para o México, para o primeiro e o terceiro trimestres entre 2009 e 2017.

PERÍODO	TAXA (US$)	MARGEM DE TAXA DE CÂMBIO (%)	CUSTO TOTAL (%)	CUSTO TOTAL (USD)
2009 1T	9,10	2,21	6,76	13,52
2009 3T	8,24	1,73	5,84	11,69
2010 1T	10,99	1,93	7,42	14,85
2010 3T	10,84	1,31	6,73	13,46
2011 1T	8,22	1,37	5,48	10,96
2011 3T	7,80	2,07	5,97	11,93
2012 1T	7,75	1,90	5,78	11,55
2012 3T	11,44	1,54	7,26	14,52
2013 1T	7,25	1,66	5,29	10,57
2013 3T	5,97	1,43	4,41	8,82
2014 1T	6,22	1,09	4,20	8,40
2014 3T	6,00	1,48	4,48	8,96
2015 1T	5,76	1,55	4,43	8,86
2015 3T	5,90	2,64	5,59	11,18
2016 1T	6,04	2,07	5,09	10,18
2016 3T	6,04	3,33	6,35	12,71
2017 1T	5,57	1,88	4,67	9,33
2017 3T	5,14	1,90	4,47	8,94

Fonte: Banco Mundial.
Dados de várias instituições financeiras foram consultados para realizar as médias, embora nem todas tenham fornecido informação para todos os trimestres. Foram consideradas transferências feitas por internet, diretamente em uma unidade física da instituição, ou por *call-center*. As seguintes instituições foram consultadas: Bancomer Transfer Services, Bank of America, Barri International, Citibank, Delgado Travel, Dinero Seguro, Dolex Dollar Express, Giromex, Intermex, Maniflo, Moneygram, Order Express, Orlandi Valuta, Remitly, Ria, Sigue, Small World FS-Choice, Viamericas, Vigo, Wells Fargo, Western Union, Xoom.

Claramente, há uma diminuição considerável do valor de US$16,02, coletado por Manuel Orozco em 2002. Realizando uma média simples do custo total de uma transferência no período 2009-2017, compreendendo apenas o primeiro e o terceiro trimestre, se tem um valor de US$11,13. Muitas são as possibilidades para tal diminuição e a explicação destes motivos obrigaria a realizar uma pesquisa estatística mais aprofundada, ou até especulativa. No entanto, é importante esclarecer que em alguns períodos de análise destes dados, algumas instituições realizaram preços promocionais específicos, assim diminuindo o preço médio do custo de transação. Da mesma maneira, algumas instituições, como a Bancomer Transfer Services e a Dinero Express se recusaram a divulgar suas taxas de câmbio para alguns períodos, como o primeiro trimestre de 2011, por exemplo. Assim sendo, o Banco Mundial compilou a

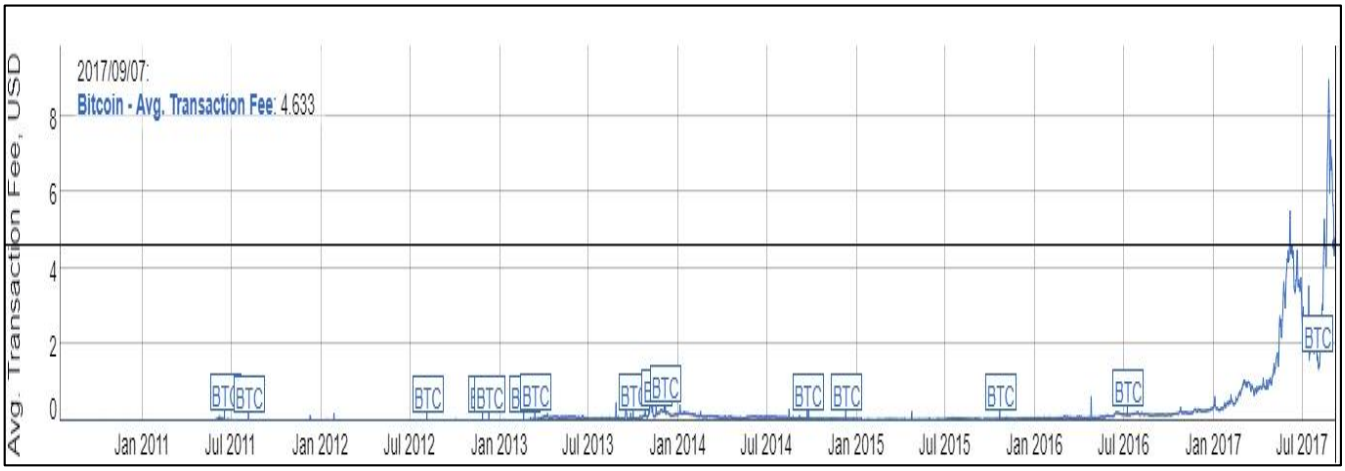
informação e registrou como “taxa 0%”, mas isto não significa necessariamente que houve isenção desta taxa.

Mesmo com a diminuição da taxa média de custo de transação, a oscilação desta taxa é consideravelmente alta. Por exemplo, a partir do terceiro trimestre de 2013, parece ocorrer um movimento descendente do preço da taxa de transação. Porém, no terceiro trimestre de 2016, esta taxa volta a ter um valor similar ao primeiro e terceiro trimestre de 2011. Isto indica que, mesmo após a entrada de mais instituições no mercado o preço continua a se manter relativamente instável, podendo dificultar a situação do imigrante que busca enviar remessas de dinheiro para seu país de origem.

Mesmo com uma taxa média de transação mais barata, a oscilação de preço antes discutida no modelo tradicional de pagamentos, não apenas se repete com o bitcoin, como se agrava de maneira contundente.

Pelo recente aumento de demanda por bitcoins, os custos de transação têm aumentado de maneira vertiginosa. Esta consequência se explica pela relação de oferta e demanda entre os consumidores e mineradores de bitcoin. O aumento da quantidade de indivíduos interessados em possuir bitcoins não tem sido acompanhado pelo ritmo de produção dos mineradores. O incremento da demanda por transações mais rápidas incentiva os mineradores a elevarem as taxas de mineração atreladas a cada transferência. Visto que quem define a taxa que é paga por transação é o próprio usuário, os mineradores passam a priorizar a programação de transações maiores, deixando de lado as transações menores, onde pagar um alto custo de transferência não faz sentido. A Figura 6 apresenta a evolução do custo de transação, em dólares americanos de uma transferência de bitcoins, desde a origem da moeda até 7 de Setembro de 2017:

Figura 6: Evolução do custo de transação médio para uma transferência de bitcoin.



Fonte: www.bitinfocharts.com

Este problema confronta diretamente um dos principais propósitos da introdução do bitcoin: a inserção de indivíduos de pouco poderio financeiro, negligenciados pelas instituições financeiras tradicionais, no mundo dos meios de pagamento. Por força de mercado, estes indivíduos ainda se veriam impossibilitados de ter acesso fluído ao meio digital de pagamentos. O crescimento exponencial das taxas de transação surge como ameaça para a realização de microtransações e consequentemente, para a introdução do bitcoin na sociedade leiga.

Utilizando a casa de câmbio de bitcoins com maior volume no Brasil, Foxbit, como referência, é possível visualizar o impacto das novas taxas nas transferências de fundos. Para realizar uma transferência de R$10,00, o custo de transação no dia 3 de Setembro de 2017, era de ฿0,00045, ou R$7,87, à taxa de câmbio do mesmo dia. No mesmo momento, para realizar uma transferência de R$10.000,00, o custo de transferência era o mesmo. Isto pode vir a se tornar um problema quanto à questão da popularidade do bitcoin como meio de troca factível para a realização de transações esporádicas do cotidiano.

Surda (2014), no entanto, defende que ver apenas a redução do custo de transação é negligenciar o potencial da tecnologia, proclamando que as facilidades que o bitcoin oferece, atrelado à rede *blockchain*, podem tornar atividades cotidianas como serviços de advocacia e contabilidade, por exemplo, obsoletos. Porém, admite a falta de casos maduros e práticos na realidade que corroborem esta posição.

5.3 A QUESTÃO DOS CUSTOS DE TRANSAÇÃO DO BITCOIN COM A TEORIA DE KEYNES

Como comentado anteriormente, no capítulo 2, John Maynard Keynes considerava os custos logísticos de uma transação como pilar fundamental da constituição da reserva de valor de uma moeda.

No contexto utilizado por Keynes, era também considerado o custo de estoque de uma *commodity*. Não é o caso do bitcoin, visto que as criptomoedas são informações digitais que percorrem a rede da internet. No entanto, existe uma força por trás da realização das transferências do bitcoin, o *proof of work* precisa ser realizado por um indivíduo ou grupo de indivíduos, os quais exigirão uma remuneração em troca deste trabalho que, neste caso, são os mineradores. Já foi discutido o conflito de interesses entre mineradores e usuários da rede e a influência que eles têm nos custos de transação.

Para Keynes, a ideia de que o dinheiro seja mais estável do que uma *commodity* reside no fato de que os salários são mais estáveis em termos de dinheiro do que em termos de *commodity*. Ao supor um contexto onde os salários fossem mais estáveis lastreados em *commodities* do que em dinheiro, Keynes (1936, p. 150) diz:

> Qual seria a situação se os salários possuíssem uma expectativa de serem mais fixos em termos de uma ou mais *commodities* que não dinheiro, do que em termos do dinheiro em si? Tal expectativa exige não só que os custos da *commodity* em questão sejam relativamente constantes em termos de unidade de salário no curto e no longo prazo, mas também que qualquer ganho sobre o preço de demanda pode ser efetivado sem nenhum custo excessivo, ou seja, que seu prêmio de liquidez exceda seus custos logísticos. Se uma *commodity* pode ser vista satisfazendo essas condições, com certeza, poderia ser colocada como uma rival ao dinheiro.

Em um contexto onde o bitcoin ainda não se consolidou como uma moeda de características estáveis, seja por condições de preço ou de custo de transação, encontram-se empecilhos para equiparar a criptomoeda ao dinheiro corrente emitido pelos bancos centrais.

A segurança que o dinheiro estatal garante, ao menos no sentido da estabilidade de preço, por ora, parece fazer do bitcoin uma moeda apoiada mais por instintos ideológicos e especulativos do que por motivos lógicos, considerando a sua breve história.

O mesmo ocorre com a questão dos custos de transação. Embora os intermediários responsáveis pelas transferências de dinheiro existam em um número escasso e com funções limitadas, a volatilidade do custo da transferência de bitcoins surge como uma ameaça à ideia original de Satoshi Nakamoto, sendo que desta vez a ameaça não parece surgir tanto pelo lado da desconfiança da população e mais pelo elo oposto da cadeia: os mineradores de bitcoin.

5.4 ENTRADA DE NOVOS PLAYERS

A estratégia descentralizada pela qual o bitcoin opera poderia facilitar o desenvolvimento de mercados financeiros que hoje se encontram em estado precário. Países com recursos escassos, onde a ideia de possuir uma conta bancária é algo utópico, poderiam se ver agraciados com a expansão das criptomoedas. Bastaria ao indivíduo ter acesso a Internet para conseguir adentrar ao mundo dos meios de pagamento, do qual por tanto tempo se viu marginalizado.

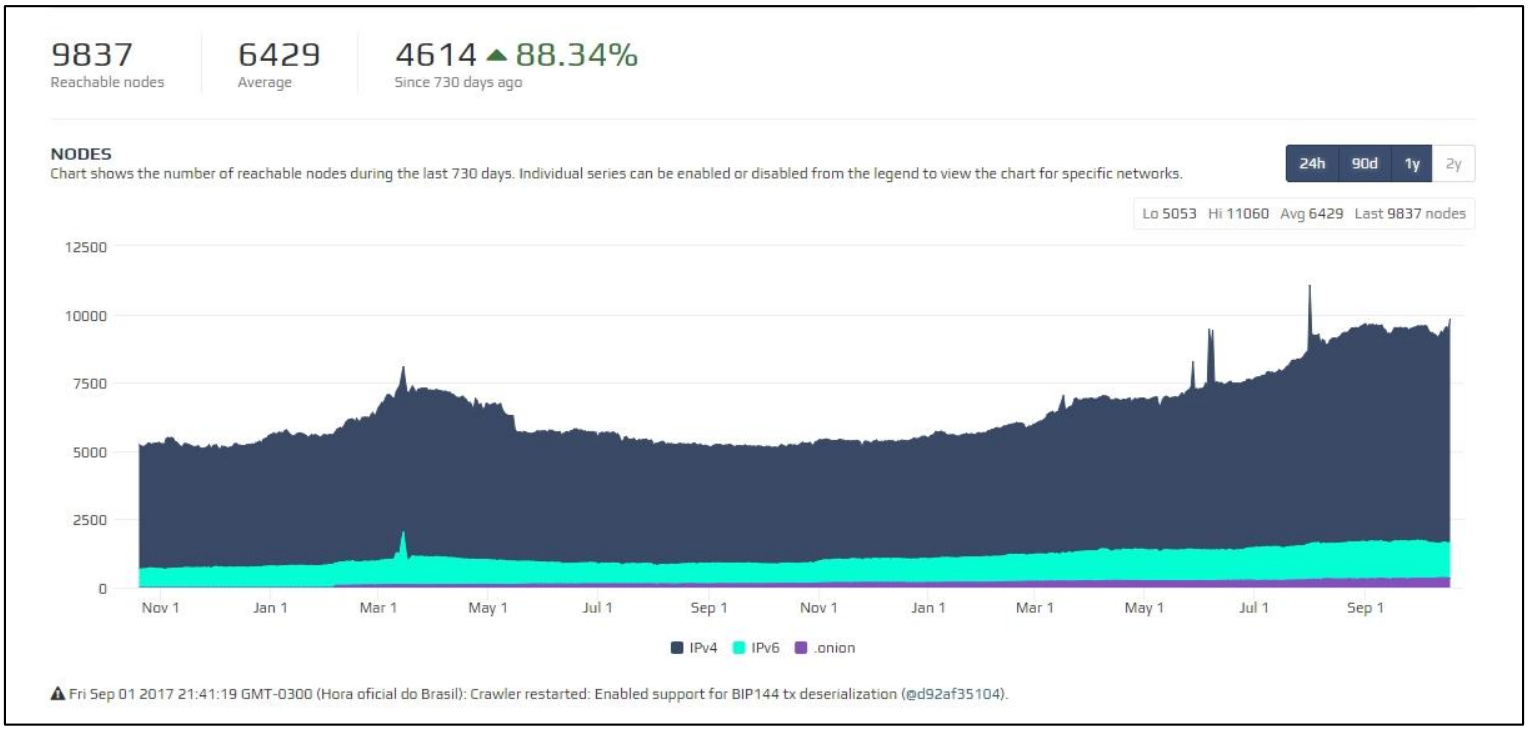
Medir o impacto que a introdução da tecnologia teria sobre as comunidades mais carentes, no momento, é entrar no campo da especulação. No entanto, não impede que o assunto passe a, pelo menos, ser assunto de pesquisas mais profundas. Kingombe (2016) aponta para o fato do evidente interesse por bitcoins no continente africano. Start-ups como Beam e Kitina, em Gana, e BitPesa, no Quênia, surgem como exemplos de empresas que facilitam as remessas de dinheiro enviadas a esses países, transformando bitcoins nas moedas locais.

Um dos riscos que a manutenção do ideal descentralizado do bitcoin sofre é que a concentração das *mining pools* se reduza a um pequeno número de agentes. Para evitar esta formação de cartel, é necessária a existência de *nodes* que assegurem a independência da rede.

Através do site https://bitnodes.earn.com/, é possível quantificar o número total de *nodes* ativos no planeta. Esta alta volatilidade em um âmbito tão importante como a estabilidade da rede, tem gerado dúvidas[14] quanto à permanência do protocolo como um mecanismo independente e de simples utilização. A seguir, a Figura 8 mostra essa volatilidade:

[14] No artigo *"Ethereum Now Has Three Times More Nodes Than Bitcoin",* publicado no site www.trustnodes.com no dia 31 de Maio de 2017, é discutida a diferença de *nodes* entre a rede Bitcoin e a Ethereum. Segundo o artigo, um intenso debate para decidir se o tamanho do bloco do bitcoin deve aumentar ou não, tem feito com que a proliferação dos *nodes* se veja entravada. No entanto, também comenta que a adoção do Ethereum para uma série de tentativas de empreendimentos e projetos alavancou a necessidade de nodes para esta criptomoeda, enquanto que o bitcoin, por ter tido uma redução de participação em empreendimentos, têm se visto menos cobiçado por agentes importantes do mercado, reduzindo seu aumento de *nodes*.

Figura 7: Acompanhamento de *nodes* ativos entre Novembro de 2015 e Outubro de 2017

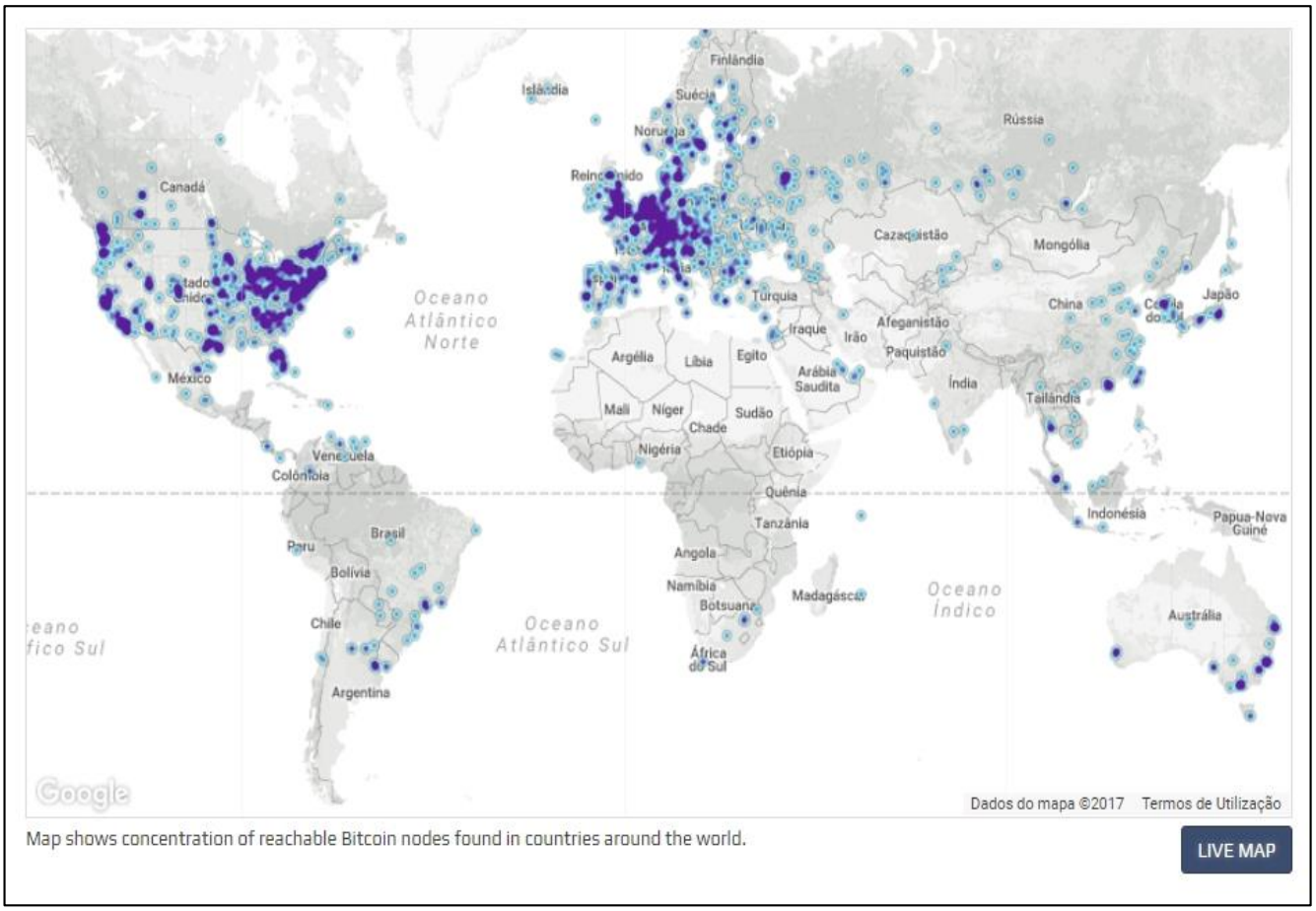


Fonte: www.bitnodes.com

Como apontado no artigo "*What Are Bitcoin Nodes and Why do We Need Them?*", publicado no site www.coindesk.com no dia 9 de Maio de 2014, de autoria de Daniel Cawrey, a volatilidade da atividade dos *nodes* é um motivo de preocupação, visto que existe pouco incentivo para que os indivíduos usem seus computadores para tal atividade. Isto pode ir de frente contra o ideal participativo do bitcoin, visto que justamente nas áreas mais precárias do planeta, como o continente africano, onde o bitcoin poderia ajudar milhões de pessoas a terem contato com recursos financeiros, é onde se encontra a maior ausência de *nodes*. A alta concentração dos *nodes* na América do Norte pode fazer com que a rede se fragilize nas áreas onde poderia ter maior impacto. Esta concentração é evidenciada na Figura 8.

Um sistema cujo principal discurso é o da descentralização e eficiência, ao se ver em um contexto de instabilidade e concentração excessiva, pode vir a passar uma mensagem desagradável a seus apoiadores, colocando em risco a viabilização do sistema como um protocolo confiável para realizar operações.

Figura 8: Concentração de *nodes* ao redor do mundo em Novembro de 2017.



Fonte: https://bitnodes.earn.com/

6 CONCLUSÃO

É interessante perceber como as ideias que Hayek e White tinham de moedas privadas conseguem se materializar parcialmente nas criptomoedas, uma espécie de ativo que não estava perto de existir à epoca das respectivas publicações dos autores sobre o tema, que foram debatidas nesta monografia. Ao mesmo tempo, características das criptomoedas como as questões dos custos de transação e volatilidade do preço, conseguem se relacionar às ideias transmitidas por Keynes, autor com visões opostas às de Hayek e White. Tanto para Keynes quanto para White, o custo de transação e de armazenamento de um bem estava diretamente relacionado à sua capacidade de conservar valor.

Uma moeda que se julgasse eficiente precisaria ser estável e de fácil transmissão. Outro ponto importante exposto, o surgimento do bitcoin como uma moeda privada, corrobora as ideias de Hayek, onde um mercado livre de emissores de moeda obrigaria cada emissor a oferecer um diferencial interessante para seu ativo como via para absorver uma parcela maior do mercado.

Acompanhar a cronologia das criptomoedas permite ter uma visão mais ampla do contexto em que elas surgem e se inserem. Ao aparecerem como instrumento de manifestação cultural e econômica contrária ao *establishment* corrente, suas virtudes e fraquezas ficam mais aparentes. Ao tempo que aparecem como uma solução objetiva para dificuldades corriqueiras do sistema financeiro internacional, como a facilidade para realizar transferências, também se mostram alvos de mera especulação financeira, como foi exposto no caso da ZCash. Não é possível delinear claramente até onde as criptomoedas são uma solução ou apenas um meio de angariar lucros. Esta é uma análise cuidadosa que deve ser feita para cada criptomoeda, mas que não deveria certificar todas as criptomoedas, nem como infalíveis, nem como defeituosas.

Não obstante o conceito de dinheiro digital e de criptomoedas, em si, não seja mais uma novidade, o cenário para estas últimas ainda é bastante nebuloso e fomentará várias discussões. Desde o *b-money* até o bitcoin, houve um amplo desenvolvimento para conseguir popularizar o dinheiro digital. Contudo, pela natureza inovadora do bitcoin, ele ainda irá atrair muita desconfiança e continuará a sofrer para superar a estrutura das instituições tradicionais, como seu propósito predica. A oscilação de preço, algo ao qual o mercado já se acostumou e a instabilidade quanto à manutenção do esqueleto do protocolo do bitcoin, criptomoeda de maior fama, constituem um obstáculo importante para que esta criptomoeda compita com os meios tradicionais de pagamento e as moedas estatais.

A viabilidade das criptomoedas, talvez o ponto mais controverso sobre o tema, se mantém como uma interrogação para a maior parte dos agentes econômicos, uma vez que a estrutura delas ameaça a confiança até da parcela de usuários mais entusiasmada com os ideais delas. Mesmo se passando em 2014, o caso da perda de bitcoins da *exchange* Mt. Gox permanece como um fantasma que assombra a materialização das criptomoedas como objeto definitivo de reserva de valor, unidade de conta e meio de troca.

O problema de uma possível concentração de *mining pools* pode vir a se tornar um empecilho comprometedor, visto que o bitcoin é fundamentado em ideias descentralizadoras, onde a ausência do intermediário, mais do que desnecessária, é imprescindível. O número reduzido de *nodes*, ao afetar a confiança no bitcoin como um meio de introdução de classes sociais mais baixas ao sistema financeiro, fragiliza ainda mais seus pilares de sustentação.

O custo de transação de bitcoins, um atrativo importante da proposta, passa a fazer parte do quadro de preocupações a respeito da moeda. Uma vez que estes custos não representem uma real vantagem em relação aos métodos tradicionais, muito do valor da moeda pode se perder, incorporando desta maneira, uma variável adicional ao problema de oscilação de preço da moeda. Ao confrontar esta fragilidade da moeda com o discurso elencado por Keynes, se encontra uma dificuldade de reconhecer o bitcoin como uma moeda capaz de ser inserida no mercado.

Além dos problemas internos do protocolo, é impossível negligenciar a influência que as autoridades governamentais podem ter sobre o futuro das criptomoedas. O componente *underground* das criptomoedas ainda as torna relativamente imunes aos aspectos regulatórios. Apesar disso, assumindo o pressuposto de que elas conseguirão ser introduzidas no mercado de maneira mais abundante, é de se esperar um confronto com regulamentações estatais de maneira muito mais aberta e clara.

Se a maioria dos governos ainda não tomou uma postura estruturada a respeito de como se comportar com a tecnologia *blockchain*, as instituições financeiras já olham para ela com outra visão. Como exposto na monografia, existe uma preocupação institucionalizada com os mecanismos modernos de transferências de fundos por parte dos grandes bancos. Investimentos em projetos envolvendo tecnologia *blockchain* já estão sendo realizados e isso não se restringe a instituições financeiras. No entanto, menções e até mesmo ataques fortes ao bitcoin, por exemplo, permanecem sendo a ordem constante nos comunicados dos grandes bancos, apontando uma postura favorável à tecnologia *blockchain*, mas contrária à formalização de moedas privadas digitais.

Assumir uma posição institucionalizada a favor ou contrária às criptomoedas é entrar em um campo muito arriscado, onde a especulação surge como pilar de sustentação da ideia, comprometendo o estudo da viabilidade prática do projeto. Diferentemente da tecnologia *blockchain*, que dá sinais de maior solidez, as criptomoedas ainda permanecem em um estágio muito primordial, falhando em pressupostos teóricos e técnicos que as credenciariam como componentes ativos do cotidiano dos cidadãos. Todavia, as criptomoedas não têm obtido espaço de destaque nas discussões por mero acaso; suas premissas merecem ser discutidas com maior afinco, e se espera que esta monografia seja capaz de contribuir para um estudo mais amplo e um debate mais aberto a respeito de suas possibilidades e sua viabilidade.

REFERÊNCIAS

AKHTAR, Tanzeel. **Bitcoin Is Attracting Serious Skeptics Despite Rising Euphoria:** Bitcoin has become mainstream and impossible to ignore. But there are still haters.. 2017. Disponível em: <https://www.thestreet.com/story/14269758/1/bitcoin-attracts-skeptics-despite-rising-popularity.html>. Acesso em: 3 out. 2017.

ALTHAUSER, Joshua. **Australian Move to Legalize Bitcoin Attracts Gold and Bullion Investor.** 2017. Disponível em: <https://cointelegraph.com/news/australian-move-to-legalize-bitcoin-attracts-gold-and-bullion-investor>. Acesso em: 12 out. 2017.

BAKER, James C.; BYLER, Ezra U.. S.W.I.F.T.: A Fast Method to Facilitate International Financial Transactions: A Fast Method to Facilitate International Financial Transactions. **Journal Of World Trade,** v. 17, n. 5, p.458-465, 1983.

BEAUCHAMP, Kenneth George. **A history of telegraphy: its technology and application.** Londres: The Institution Of Engineering And Technology, 2008.

BLUNDELL-WIGNALL, Adrian. The Bitcoin Question. **OECD Working Papers On Finance, Insurance And Private Pensions: Currency versus Trust-less Transfer Technology,** [s.l.], v. 37, p.1-21, 16 jun. 2014. Organisation for Economic Co-Operation and Development (OECD). http://dx.doi.org/10.1787/5jz2pwjd9t20-en.

BOURI, Elie et al. On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier? **Finance Research Letters,** Amsterdam, v. 20, p.192-198, fev. 2017.

CARVALHO, Fernando J. Cardim de. Keynes on Expectations, Uncertainty and Defensive Behavior. **Brazilian Keynesian Review,** Belo Horizonte, v. 1, n. 1, p.44-55, jan./jun. 2015.

CASHLESS ECONOMY LEADS TO KNOWLEDGE ECONOMY THROUGH KNOWLEDGE MANAGEMENT. Massachusetts: Global Journals Inc, v. 16, n. 8, 2016. Disponível em: <http://www.journalofbusiness.org/index.php/GJMBR/article/view/2110/2012>. Acesso em: 29 mar. 2017.

CAWREY, Daniel. **What Are Bitcoin Nodes and Why Do We Need Them?** 2014. Disponível em: <https://www.coindesk.com/bitcoin-nodes-need/>. Acesso em: 22 set. 2017.

CHARLES BRENNAN (Reino Unido). Credite Suisse. **Blockchain:** The Trust Disrupter. 2016. Disponível em: <https://www.finextra.com/finextra-downloads/newsdocs/document-1063851711.pdf>. Acesso em: 11 set. 2017.

CNBC LLC. **India's rupee restrictions are boosting demand for bitcoin.** 2017. Disponível em: http://www.cnbc.com/2016/11/15/india-rupee-restriction-boost-bitcoin-digital-currency.html. Acesso em: 23 abr. 2017

DAI, Wei. B-money. Disponível em: <http://www.weidai.com/bmoney.txt> . Acesso em: 12 setembro 2017.

DNALEOR. **On Fungibility, Bitcoin, Monero and why ZCash is a bad idea.** 2016. Disponível em: <https://steemit.com/bitcoin/@dnaleor/on-fungibility-bitcoin-monero-and-why-zcash-is-a-bad-idea>. Acesso em: 02 out. 2017.

FRIEDMAN, Milton; SCHWARTZ, Anna J.. Has Government Any Role in Money? In: SCHWARTZ, Anna J.. **Money in Historical Perspective.** Chicago: University Of Chicago Press, 1987. Cap. 12. p. 289-314.

GERVAIS, Arthur et al. Is Bitcoin a Decentralized Currency? **Ieee Security & Privacy,** [s.l.], v. 12, n. 3, p.54-60, maio 2014. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/msp.2014.49.

GLOBALSIGN - GMO INTERNET GROUP. **What is public-key cryptography?:** A look at the encryption algorithm and its security benefits. Disponível em: <https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/>. Acesso em: 03 set. 2017.

HAYEK, Friedrich. **Denationalisation of Money:** The Argument Refined**:** An Analysis of the Theory and Practice of Concurrent Currencies. 3. ed. Londres: The Institute Of Economic Affairs, 1990. Disponível em: <https://mises.org/sites/default/files/Denationalisation%20of%20Money%20The%20Argument%20Refined_5.pdf> Acesso em: 29 mar. 2017.

KEYNES, John Maynard. The General Theory of Employment. **The Quarterly Journal Of Economics.** Oxford, p. 209-223. fev. 1937.

KEYNES, John Maynard. **The General Theory of Employment, Interest, and Money.** Londres: Palgrave Macmillan, 1936. 472 p.

KINGOMBE, Christian Kitenge Moembo. **The Quest to Lower High Remittance Costs to Africa: A Brief Review of the Use of Mobile Banking and Bitcoins. 2nd Version.** Geneva: Graduate Institute Of International And Development Studies (IHEID), 2016.

KHATWANI, Sudhir. **What is a Bitcoin Hash?** 2017. Disponível em: <https://coinsutra.com/bitcoin-hash/>. Acesso em: 28 set. 2017.

LÁNSKÝ, Jan. Analysis of Cryptocurrencies Price Development. **Acta Informatica Pragensia,** [s.l.], v. 5, n. 2, p.118-137, 2016. University of Economics. http://dx.doi.org/10.18267/j.aip.89.

MANKIW, Nicholas Gregory. **Brief Principles of Economics.** 7. ed. Stamford: Cengage Learning, 2015.

MARIAN, Omri Y.. Are Cryptocurrencies 'Super' Tax Havens? **Michigan Law Review First Impressions,** Ann Arbor, Mi, v. 112, n. 38, p.38-48, out. 2013.

MAY, Timothy C.. **The Crypto Anarchist Manifesto.** 1992. Disponível em: <https://www.activism.net/cypherpunk/crypto-anarchy.html>. Acesso em: 10 out. 2017.

MCCALLUM, Bennett T.. The Bitcoin Revolution. **Cato Journal,** Washington, Dc, v. 35, n. 2, p.347-356, spring/summer 2015.

MONAGHAN, Angela. **Bitcoin is a fraud that will blow up, says JP Morgan boss:** Jamie Dimon claims cryptocurrency is only fit for use by drug dealers, murderers and people living in North Korea. 2017. Disponível em: <https://www.theguardian.com/technology/2017/sep/13/bitcoin-fraud-jp-morgan-cryptocurrency-drug-dealers>. Acesso em: 17 set. 2017.

MURDOCH, Steven J.; ANDERSON, Ross. Security Protocols and Evidence: Where Many Payment Systems Fail. **Financial Cryptography And Data Security,** [s.l.], p.21-32, mar. 2014. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-662-45472-5_2.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 17 set. 2017.

P2POOL. Disponível em: <https://en.bitcoin.it/wiki/P2Pool>. Acesso em: 15 set. 2017.

PROOF of Work. Disponível em: <https://en.bitcoin.it/wiki/Proof_of_work>. Acesso em: 01 set. 2017.

RID, Thomas. **The Cypherpunk Revolution.** 2016. Disponível em: <http://projects.csmonitor.com/cypherpunk>. Acesso em: 7 set. 2017.

SCHWARTZ, Anna J.; FRIEDMAN, Milton. **Money in Historical Perspective.** Chicago: University Of Chicago Press, 1987. 442 p.

SCOTT, Susan V.; ZACHARIADIS, Markos. Origins and development of SWIFT, 1973–2009. **Business History,** [s.l.], v. 54, n. 3, p.462-482, jun. 2012. Informa UK Limited. http://dx.doi.org/10.1080/00076791.2011.638502.

SINGAPORE MANAGEMENT UNIVERSITY (Cingapura) (Comp.). **Bitcoins, block chains, and mining pools.** 2014. Disponível em: <http://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=1241&context=pers>. Acesso em: 09 set. 2017.

ŠURDA, Peter. The Origin, Classification and Utility of Bitcoin. **Ssrn Electronic Journal,** [s.l.], maio 2014. Elsevier BV. http://dx.doi.org/10.2139/ssrn.2436823.

SWAN, Melanie. **Blockchain:** Blueprint for a New Economy. O'Reilly Media, 2015.

TEO, Ernie. **Bitcoins, block chains, and mining pools.** Bras Basah, Cingapura: Singapore Management University, 2014.

ULRICH, F. Bitcoin: a moeda na era virtual. São Paulo. Instituto Ludwig von Misses Brasil. 2014

VAN ALSTYNE, Marshall. Why Bitcoin Has Value. **Communications Of The Acm,** [s.l.], v. 57, n. 5, p.30-32, 1 maio 2014. Association for Computing Machinery (ACM). http://dx.doi.org/10.1145/2594288.

WHITE, Lawrence H.. The Market for Cryptocurrencies. **Ssrn Electronic Journal,** [s.l.], p.14-45, 2014. Elsevier BV. http://dx.doi.org/10.2139/ssrn.2538290.

WHITE, Lawrence H.. **The Theory of Monetary Institutions.** Oxford: Blackwell Publishers Inc., 1999.

WOLFF-MANN, Ethan. **What Bitcoin needs to do to become a real currency.** 2017. Disponível em: <https://finance.yahoo.com/news/bitcoin-needs-become-real-currency-134831445.html>. Acesso em: 28 ago. 2017.

YERMACK, David. Is Bitcoin a Real Currency? An economic appraisal. **Nber Working Paper No. 19747,** [s.l.], p.1-22, dez. 2013. National Bureau of Economic Research. http://dx.doi.org/10.3386/w19747.